Survey on Network Slicing for Internet of Things Realization in 5G Networks

Shalitha Wijethilaka, *Student Member, IEEE*, and Madhusanka Liyanage, *Senior Member, IEEE*,

***Abstract*—Internet of Things (IoT) is an emerging technology that makes people's lives smart by conquering a plethora of diverse application and service areas. In near future, the fifth-generation (5G) wireless networks provide the connectivity for this IoT ecosystem. It has been carefully designed to facilitate the exponential growth in the IoT field. Network slicing is one of the key technologies in the 5G architecture that has the ability to divide the physical network into multiple logical networks (i.e., slices) with different network characteristics. Therefore, network slicing is also a key enabler of realisation of IoT in 5G. Network slicing can satisfy the various networking demands by heterogeneous IoT applications via dedicated slices. In this survey, we present a comprehensive analysis of the exploitation of network slicing in IoT realisation. We discuss network slicing utilisation in different IoT application scenarios, along with the technical challenges that can be solved via network slicing. Furthermore, integration challenges and open research problems related to the network slicing in the IoT realisation are also discussed in this paper. Finally, we discuss the role of other emerging technologies and concepts, such as blockchain and Artificial Intelligence/Machine Learning (AI/ML) in network slicing and IoT integration.**

***Index Terms*—Network slicing, IoT, 5G, SDN, NFV, network architecture, latency, reliability.**

I. INTRODUCTION

INTERNET has evolved over the last four decades, from simple peer-to-peer networks to an advance IoT ecosystem (Figure 1). With the ubiquitous utilisation of IoTs, everything around us is becoming smart. It is possible to connect people and things at any time from any place with network access, to receive information of the thing, to operate the thing or even both, to make the life of the mankind easier [1]. The number of connected devices proliferates exponentially. According to Machina research, it is expected that the number of connected devices will be 27 billion by 2024 [2]. Diversity of these IoT applications will also expand from simple smart home solutions to mission-critical health care systems [3]. These application scenarios demand various performance requirements such as low latency, ultra-reliability, high security and high data rates.

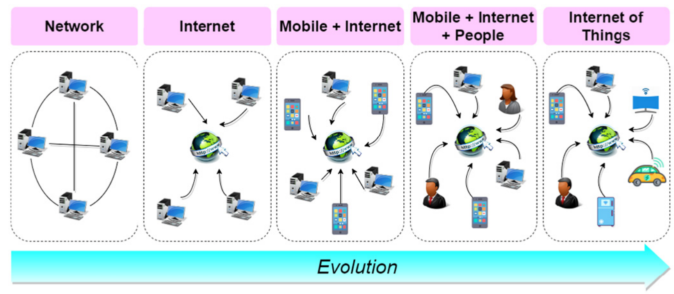

Fig. 1. Evolution of the Internet.

Most of these connected devices will use the wireless infrastructure to communicate. However, the existing wireless infrastructure is not able to handle the rapid growth of IoT connections along with typical mobile connections. Moreover, such networks are incapable of satisfying the heterogeneous QoS requirements for different IoT application scenarios. As a solution, the 5G architecture is designed with the aid of various new technologies to handle these requirements.

Software Defined Networking (SDN), Network Function Virtualization (NFV), Multi-access Edge Computing (MEC) and network slicing are some of the predominant technologies in 5G architecture [4]–[7]. SDN offers the ability to control the network traffic routing centrally and intelligently, using software applications [8]. Centralised control, network programmability and abstraction are the key benefits of SDN. NFV is a concept which is used to package network functions such routing, load balancing and firewalls as software applications, so that they can run on commodity and general hardware devices [9]. Tight coupling between network functions and specific hardware units was a huge bottleneck to the evolution of such network functions. This can be eliminated by using NFV. Providing cloud computing capabilities to the edge network is the main purpose of MEC technology [10]. It will minimise the network congestion on backhaul and improve the resource optimisation, user experience and the overall performance of the network [11].

Dividing the physical network into separate logical networks known as slices is called network slicing. Each slice can be configured to offer specific network capabilities and network characteristics [12]. Thus, the End-to-End (E2E) network slicing can help to deploy various 5G based services [13]–[18].

Manuscript received September 25, 2020; revised December 16, 2020 and January 26, 2021; accepted March 11, 2021. Date of publication March 22, 2021; date of current version May 21, 2021. *(Corresponding author: Shalitha Wijethilaka.)*

Shalitha Wijethilaka is with the School of Computer Science, University College Dublin, Dublin 4, D04 V1W8, Ireland (e-mail: mahadurage.wijethilaka@ucdconnect.ie).

Madhusanka Liyanage is with the School of Computer Science, University College Dublin, Dublin 4, D04 V1W8, Ireland, and also with the Centre for Wireless Communications, University of Oulu, 90014 Oulu, Finland (e-mail: madhusanka.liyanage@oulu.fi).

Digital Object Identifier 10.1109/COMST.2021.3067807

TABLE I
SUMMARY OF ACRONYMS

Acronym	Definition
3GPP	Third Generation Partnership Project
5G	Fifth Generation Wireless Network
AI	Artificial Intelligence
AR	Augmented Reality
BLE	Bluetooth Low Energy
CaPC	Cloud-aware Power Control
CPS	Cyber Physical System
C-RAN	Cloud Radio Access Network
D2D	Device-to-device
DDoS	Distributed Denial of Service
DoS	Denial of Service
E2E	End-to-end
EC	Edge Computing
eMBB	enhance Mobile Broadband
EMM	Energy-aware Mobility Management
eNodeB	Evolved Node B
ETSI	European Telecommunications Standards Institute
EU	European Union
FiWi	Fiber-enable Wireless
F-RAN	Fog Radio Access Network
GDPR	General Data Protection Regulation
ICN	Information Centric Networking
ICT	Information Communication Technology
IIoT	Industrial Internet of Things
ISG	Industry Specification Group
IoT	Internet of Things
LPWAN	Low-power Wide Area Network
LTE	Long Term Evolution
M2M	Machine-to-machine
MANO	Management and Orchestration
MEC	Multi-Access Edge Computing
MitM	Man-in-the-Middle
mmW	millimeter-Wave
MR	Mixed Reality
NB-IoT	Narrow-band IoT
NFV	Network Function Virtualization
PbD	Privacy by Design
QoE	Quality of Experience
QoS	Quality of Service
RAN	Radio Access Networks
RAT	Radio Access Technology
RNC	Radio Network Controller
SDN	Software Defined Networking
SDP	Software Defined Privacy
UAV	Unmanned Aerial Vehicles
UE	User Equipment
V2V	Vehicle to Vehicle
V2X	Vehicle to Everything
VM	Virtual Machine
VNF	Virtual Network Function
VR	Virtual Reality
VRARA	Virtual Reality/Augmented Reality Association
WIoT	Wearable Internet of Things
WLAN	Wirless Local Area Networking
WSN	Wireless Sensor Network
WAN	Wide Area Networking
WAP	Wireless Access Point

SDN and NFV can be identified as key enabling technologies for network slicing realisation in 5G networks [19].

A. Role of Network Slicing for IoT

In a nutshell, 5G network architecture is designed to support three main fundamental service classes: enhanced Mobile BroadBand (eMBB), massive Machine Type Communications (mMTC) and Ultra-Reliable Low-Latency Communications (URLLC) [12]. Each service class has a diverse set of network requirements. Therefore, the creation of an E2E network slice for each service scenario is needed, to allocate required resources to fulfill the such requirements.

Similarly, different IoT applications demand different networking requirements. For instance, more than 99.99% reliability level and less than 1 ms E2E latency are required for mission-critical communication IoT use cases. 10^{-9} packet loss rate and E2E latency range of 250 μs to 10 ms are required factory automation applications [20]. Such diverse requirements of different IoT applications can be fulfilled by allocating a dedicated E2E network slice for each application (Figure 2).

The Network Slice as a Service (NSlaaS) concept allows operators to create customised network slices for their customers as a service. This generates a new business model for Mobile Network Operators (MNOs) [31], [32]. Moreover, an E2E network slicing framework that has the ability to horizontally slice computation and communication resources was proposed in [33] for supporting vertical industry applications.

Network slicing improves the efficiency of resource utilisation by dynamically adjusting network resources between the slices. It is possible to implement autonomous systems for such resource allocations and dynamic adjustment of resources [34]. This method can be used to improve the scalability of future IoT applications.

High security and privacy for sensitive IoT applications, such as healthcare, can be achieved through the slice isolation. For instance, a secure service-oriented authentication framework has been proposed by Ni *et al.* for the realisation of IoT services in 5G networks through fog computing and network slicing [35]. Since IoT devices are generally resource-constraint, they are highly vulnerable to attacks. The rapid growth in the number of IoT devices and pervasiveness are also attracting many attackers to the IoT ecosystem [36]. An adversary can easily dominate IoT devices and can lead them to generate Distributed Denial-of-Service (DDoS) attacks to the network. The severity of these kinds of attacks can be minimised through isolating IoT applications using network slicing. Also, dynamic allocation of idle resources to the victimised network slice is possible to keep the service without any degradation during an attack.

B. Paper Motivation

IoT expands its roots over each and every field by permuting unintelligible dumb items into smart things over the last few years. A large number of vertical industries are engaged in developing smart solutions at a very high speed and the community rapidly adopts these into their lifestyle. Multiple surveys related to IoT have been conducted during the past few years over several subareas. Standardisation, security, architecture, privacy, trust, visions, challenges and future research directions are some key areas that are exploited in existing surveys and researches.

Network slicing is a neoteric technology and numerous network slicing-related areas have to be investigated. The standardisation of network slicing is still ongoing by telecommunication organisations. Though it is possible to find surveys and researches associated with network slicing within the past

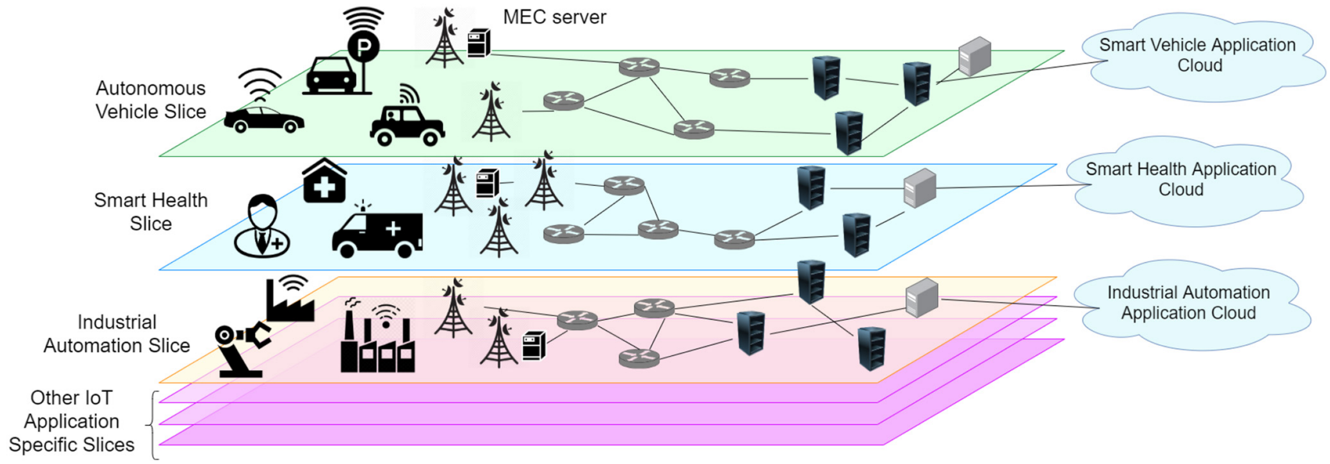

Fig. 2. E2E Network Slicing.

TABLE II
SUMMARY OF IMPORTANT SURVEYS ON NETWORK SLICING

Ref.	Main contribution	Relevance to IoT
[21]	Comprehensive review on network slicing and network slicing enabling technologies are provided. Standardization efforts, industrial projects that accelerate network slicing usage, challenges and research directions are discussed.	No explicit focus on IoT.
[22]	Latest status of 3GPP standardization, overview of solutions for problems introduced by complexity of network slicing and future research areas discussed.	No explicit focus on IoT.
[23]	Discussion about network slicing architecture and technologies related with network slicing provided.	No explicit focus on IoT.
[24]	Discussed use cases of smart grid system using network slicing.	Discussed only one IoT application scenario.
[19]	End to End network slicing with concepts, technologies and solutions discussed. In addition use cases and open research directions, are discussed.	Generally discussed IoT.
[25]	Network slicing concept, aspects that enable network slicing realization and open research issues, are analyzed.	No explicit focus on IoT
[26]	Reviewed the state of the art in network slicing. A framework has presented and evaluated the maturity of current proposals. Identified open research problems	No explicit focus on IoT.
[27]	Analyzed resource allocation algorithms in 5G network slicing and discussed open research problems	No explicit focus on IoT.
[28]	Issues in allocation, isolation, guaranteeing the intraoperability of the resources between slices discussed. Provided new open research topic in related with discussed issues.	Generally discussed.
[29]	Discussed about network slicing in different parameters and key requirements for network slicing to enable smart services.	Several application areas have been discussed along with network slicing.
[30]	Providing scalable cloud resources for IoT using network slicing, has been discussed. Detailed discussion on utilizing SDN and edge computing for IoT presented.	No explicit focus on utilizing network slicing in IoT.

few years, most of them tend to be conceptual rather than technical. Table II consists of a summary of existing surveys related to network slicing. Slicing architecture, technologies that support network slicing realisation, standards, security and use cases are the areas that are covered by most surveys.

In [21], they have carried out a comprehensive review of network slicing with enabling technologies, standardisation efforts, industrial projects that accelerate network-slicing usage and future research directions. The latest status of 3GPP standardisation, solutions to reduce the complexity introduced by network slicing and future research areas discussed in [22]. Network slicing architecture and some particular technologies that can be used with network slicing are discussed in [23]. Reference [24] discussed a significant use case in future IoT: smart grid, E2E network slicing with concepts, technologies, solutions and use cases are considered in [19]. The network slicing concept with aspects that support network slicing realisation is discussed in [25]. In [26], Foukas *et al.* reviewed state-of-the-art network slicing and they have presented a framework and evaluated it under the maturity of current proposals. Resource allocation algorithms are analysed in [27]. Issues in allocation, isolation, guaranteeing the inter-operability of the resources between slices discussed in [28]. Enabling smart services in future networks with network slicing and different parameters in network slicing are discussed in [29]. Future research areas of network slicing with open research problems are highlighted in [19], [21], [22], [25], [26], [28], [29].

As with the references that we could find, there is no single survey that specifically analyses the contribution of network slicing to the IoT realisation. Since network slicing is the prominent technology that reinforces IoT realisation in 5G networks, it is pertinent to analyse the associativity between network slicing and IoT, in terms of technical aspects, applications and challenges.

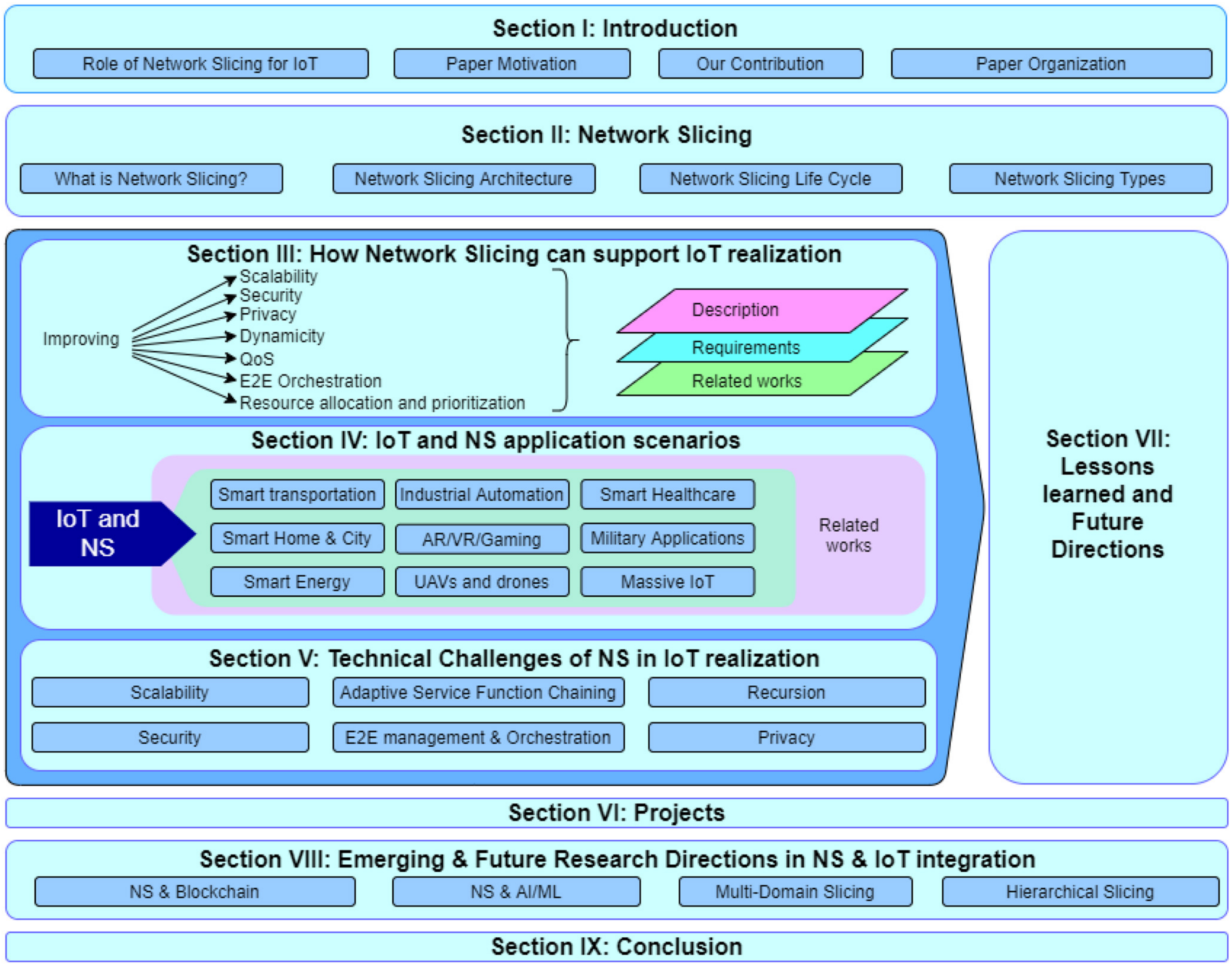

Fig. 3. Paper Organization.

C. Our Contribution

In our survey, we broadly investigate how network slicing will overcome the challenges of IoT technologies and their related applications in future networks. Since there are enough surveys related to network slicing integration technologies, such as SDN and NFV, they will not be covered in this survey. A comprehensive overview of the state-of-the-art technical aspects that can be used to IoT realisation via network slicing will be provided through the survey. The impact of the emerging technologies and concepts, such as blockchain and AI/ML, in network slicing and different IoT applications will be discussed in here. Our contribution to the IoT realisation via network slicing through this paper is enumerated as follows.

1) Technical aspects that can be improved via network slicing in the IoT realisation.
2) Detailed discussion on the utilisation of network slicing for the realisation of divergent IoT use cases with different network requirements.
3) A comprehensive analysis of the technical challenges of network slicing that will rise due to the advancement of the IoT.
4) A concise summary of the network slicing-related projects that have a impact on IoT.
5) A discussion on the impact of the emerging technologies in network slicing and IoT.
6) A pool of future research directions in applying network slicing on several IoT applications and technical aspects.

D. Paper Organization

The paper consists of nine sections and the organisation is as follows. Section II provides the background knowledge of network slicing in order to understand the concept. Section III focuses on improving the technical aspects related to IoT via network slicing. Scalability, dynamicity, security, privacy, QoS, E2E orchestration and resource allocation and prioritisation are discussed in here. Network slicing utilisation, in several IoT application areas, is described in Section IV. Section V is allocated to discuss the technical challenges of network slicing that can rise with the advancement of IoT. Network slicing-related projects are described in Section VI and Section VII is dedicated to discuss the lessons learned in each application and technical aspect with future research

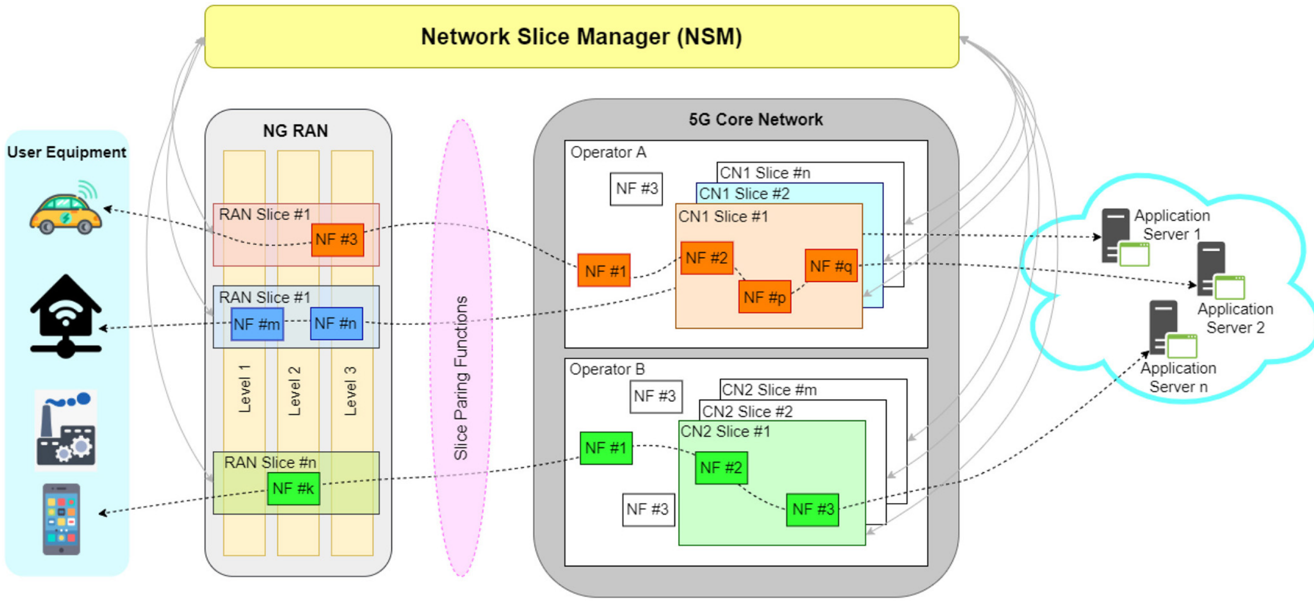

Fig. 4. Overall Network Slicing Architecture.

directions respectively. The impact of emerging technologies in the IoT realisation via network slicing is described in Section VIII. Finally, Section IX concludes the paper. Graphical representation of the paper organisation is shown in Figure 3. We included the definitions of the frequently used acronyms in Table I.

II. Network Slicing

A. What Is Network Slicing?

Future mobile networks will have heterogeneous service requirements due to the wide set of new networking services. Thus, the 'one size fits all' networking concept is not applicable for 5G and beyond. Next Generation Mobile Network(NGMN) Alliance first introduced the network slicing concept in 2015 to address the above issue. Third Generation Partnership Project (3GPP) considers network slicing as a key feature in 5G networks [11]. The concept of dividing the physical network into multiple logical networks (network slices) so that each logical network can be specialised to provide specific network capabilities and characteristics for a particular use case can be identified as network slicing [18]. 3GPP defines network slicing as a "technology that enables the operator to create networks, customised to provide optimised solutions for different market scenarios which demand diverse requirements (e.g., in terms of functionality, performance and isolation)" [37].

According to [19], network slicing is built upon seven main principles: isolation, elasticity, automation, programmability, customisation, E2E and hierarchical abstraction.

B. Network Slicing Architecture

As stated by NGMN, network slicing architecture consists of three layers: **infrastructure layer**, **network slice instance layer** and **service instance layer** [38].

- **Infrastructure layer** is responsible for providing physical or virtual resources such as storage, computing resource and connectivity.
- **Network slice instance layer** which runs over the infrastructure layer, consists of NSIs which form E2E logical network slices.
- **Service instance layer** which runs over all other layers, represents end user and business services. These services will be provided via service instances by the network operator or by a third party.

A functional network slice basically consists of two subslices: the RAN subslice, specific to Next-Generation Radio Access Network (NG RAN) and the core subslice, specific to core network. An overview of the network slicing architecture is shown in Figure 4 and it mainly consists of four segments: **RAN subslice**, **slice-paring functions**, **core subslice** and **the NSM**. Fully data flow of some particular applications throughout the network is shown in the Figure 4. A fully functional network slice is able to route and control a particular packet over the network without influencing other slices.

Multiple types of User Equipment (UE) can be connected through air interface or fixed-line interface. Thus, RAN is sliced according to different tenant requirements of each application. Radio resource management, slice specific admission control policies, the configuration rules for Control Plane (CP) and User Plane (UP) functions and UE awareness on the RAN configuration for the different services are the key design aspects for RAN slicing [39]. Separation of RAN resources can be achieved through frequency, time, code, hardware equipment, software and other dimensions [12].

RAN subslice and core subslice will be connected through slice-paring functions. Paring among RAN/core slices can be 1:1 or 1:N, e.g., a RAN slice could be connected with multiple core slices [33].

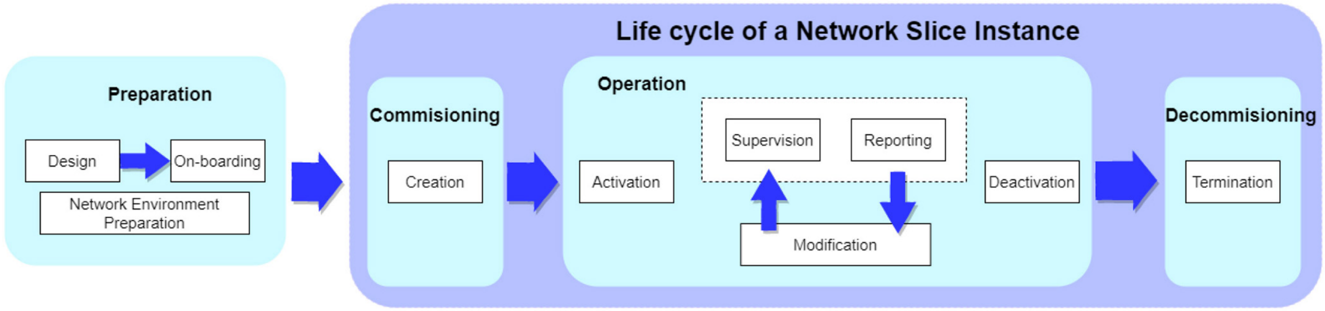

Fig. 5. Network Slicing Life Cycle.

Core network-related functionalities related to a particular application will be provided via a core slice. Core network resources can be sliced over servers, virtual machines or containers or hardware elements. Logical separation between CP and UP functions and the corresponding implemented VNFs should be considered while designing CN slices. All the operational and management tasks related to NSIs will be facilitated via the NSM.

NSM plays a key role in network slicing architecture and provides ample services. Composition and deployment of new Network Slice Templates (NSTs) is a significant service provided by NSM. NST is the blueprint of the NSIs and it is fabricated according to the particular requirements of the tenants using the network capabilities in each technical domain. NSI-related activities such as status monitoring, scale in/out and destruction are some other functionalities provided by the NSM.

A network slice consists of network functions and those network functions can be categorised as slice-specific network functions and slice-independent network functions. Since there is no consensus on selecting slice-independent network functions, this categorisation is considered as an unresolved design issue in network slicing realisation in 5G networks [40]. Due to the relative ease of implementing core NFs as software applications, core slicing is a less complex task than RAN slicing.

C. Different Types of Network Slices

Network slices can be categorised using several models: vertical and horizontal, static and dynamic and RAN and core. RAN and core slicing have been discussed earlier.

- **Vertical network slicing:** This can be defined as partitioning the network according to the use cases, whilst simplifying the traditional QoS problem. Here, each network domain will be sliced and then those slices will be paired using the slice paring functions to create the complete slice. With the advent of 5G, several new applications, such as smart wearables, Augmented Reality (AR)/ Virtual Reality (VR) and UHD video, became increasingly popular among the community and for each application, a vertical network slice can be allocated. Few vertical network slices can be identified in 4G LTE either: NB-IoT slice and MTC slice [33].
- **Horizontal network slicing:** A large amount of traffic is generated at the very edge of the network. Through edge computing and computation offloading, the generated traffic flow can be made non-uniform. This scenario can be identified as horizontal network slicing. It removes the need of high-resource requirements like computation, communication and storage in a device itself. Complex tasks that required high computation power can be handed over to the next higher layer. As an example, AR and VR devices need a very high computation capability, which cannot be provided through existing hardware that can be realised through edge computing technologies.

Vertical and horizontal network slicing is possible with static and dynamic network slicing.

- **Static network slicing:** In here, network slices will be pre-instantiated and devices need to select the slice which it is going to have the connection.
- **Dynamic network slicing:** Operators are able to dynamically design, deploy, customise and optimise the slices according to the service requirements or conditions in the network [41]. It encourages the emergence of the novel concept known as Network Slice as a Service(NSaaS).

D. Network Slice Life Cycle

NSI life cycle can be divided into four phases: **preparation**, **commissioning**, **operation** and **decommissioning** (Figure 5).

- **Preparation phase** Life cycle starts from the preparation phase and NSI does not exist in this phase. Tasks in this phase are as follows.
  - NST creation and verification.
  - Preparation of necessary network environment which is used to facilitate the NSI life cycle.
  - Capacity planning of the network slice.
  - Onboarding NSTs.
  - Evaluation of the network slice requirements.
  - Preparation of any other requirements in the network.
- **Commissioning phase:** In this phase, NSI will be created from the NST. Tasks in here:
  - Allocating the required network resources.
  - Performing the necessary configurations to facilitate the slice requirements.

  Network slice will be ready for the operation phase after this phase.
- **Operation phase:** This phase consists of multiple subtasks related to network slice instance:

  - Activation: Activating the NSI is done in here through the processes, such as diverting traffic to the slice and provisioning databases.
  - Supervision: NSI will be continuously supervised.
  - Key Performance Indicator (KPI) monitoring : NSI will be continuously monitored.
  - Modification: Upgrading NSI, reconfiguration, changes in NSI topology, association and dis-association of network functions with NSI, NSI scaling and altering NSI capacity will be handled under here.
  - Deactivation: Taking the NSI out of the active duty is done in here.
- **Decommissioning phase:**
  - Reclamation of dedicated resources.
  - Reclamation of configurations from the shared/dependent resources.

  After this phase, the NSI does not exist anymore.

III. The Role of Network Slicing in IoT Realization

This section focuses on the technical aspects that can be improved for the IoT realisation via network slicing. Improving scalability, dynamicity, security, privacy, QoS, and E2E orchestration, through network slicing, are discussed here.

A. Improving Scalability

Scalability, often a sign of stability and competitiveness, is an attribute that is used to describe the ability of a process, software, organisation, or network, to grow and manage increased demand [42]. A proper scalable network should be able to handle the influx of traffic while utilising a limited number of resources. Network slicing has been identified by 3GPP as a technology to improve the flexibility and scalability in networking systems including IoT networks [43]. Software-based network functions in network slices allow deploying network functions according to the network traffic to achieve scalability.

1) Description of the Limitation: The number of connected IoT devices will be exponentially increasing in modern telecommunication networks with heterogeneous network requirements. According to the statistics, the number of IoT devices in 2020 which is 31 billion devices, will increase to 75 billion IoT devices by 2025, and 127 new IoT connections will be established at every second [44]. This growth of IoT devices will be under myriads of new IoT based applications such as smart healthcare, smart grid, autonomous vehicles, industrial automation and AR/VR technologies. Frequent connections and disconnections of nodes of various applications with the network are possible. It might pave the way to cause performance degradation, as well as the inability to fulfill the network requirements of a diverse set of applications. To handle these recurring changes in the IoT traffic flow, the network should be scalable.

2) Benefits of Using Network Slicing: The amount of the IoT traffic flow through the network is not always the same. Due to the energy saving communication links, IoT devices operate in sleep and wake cycles. This causes network resources to be idle or over-utilised from time to time. Network slicing facilitates the dynamic allocation of idle network resources of a particular network slice to another slice that demands high resource requirements. This process improves the scalability of the IoT network and finally, it leads to enhance the network performance, increase the efficiency of resource utilisation and reduce the infrastructure cost [38].

3) Existing Slicing Based Solutions: According to the proposed existing solutions, network slicing is identified as a solution to improve the scalability of the 5G based IoT networks. In [45], they concluded that the network slicing has the potential to address diverse requirements of 5G IoT networks that finally lead to improve the scalability of future IoT applications. Their solution is more conceptual and implementations have not been provided. The presented dynamic network slicing framework to improve the scalability of fog networks in [46] needs to extend to 5G core network. Furthermore, AI/ML-based prediction algorithms can be developed to enhance resource allocation that supports improving scalability of the IoT networks.

B. Improving Dynamicity

Dynamicity describes the continuously changing nature of something. Introduction of IoT and IoT application will change the fixed nature of the traditional telecommunication networks. Dynamicity should be a key requirement for 5G and beyond network to facilitate heterogeneous IoT ecosystem and also to optimise resource utilisation.

1) Description of the Limitation: IoT requires to accomplish dynamicity of its network facilities in two main scenarios: dynamic network resource requirements of IoT applications, and rapid temporary network deployments for emergency IoT applications. The quantity of resource is approximately remains constant for a long period in most telecommunication networks. Such limited and constant resources have to be optimally utilised among heterogeneous networking applications including IoT applications. The amount of resource utilization dynamically varies according to the traffic demand which leads to resources been under-utilised or over-utilised time to time. By nature, IoT applications are extremely dynamic and their traffic patters are fluctuating constantly. Not only allocation of dedicated portions of the physical network for different IoT applications, but also dynamically change of the resource quantity of those portions according to traffic flow, are a vital requirement to operate an efficient IoT services. Moreover, IoT uses in applications such as emergency situations (floods, earthquakes) and military scenarios. Hence, rapid deployment of temporary IoT networks is required to facilitate communication requirements of such IoT applications. The solution should be fast and effortlessly deployable, and cost-effective.

2) Benefits of Using Network Slicing: Network slicing can support to eliminate the static nature of the networks to make them dynamic. Dynamic slice allocation for heterogeneous IoT applications and dynamic resource allocation between slices are two ways of improving dynamicity of the

TABLE III
KEY IoT SECURITY ATTACKS

Security attack	Description	Support from NS	Related works
DDoS attacks	Tries to overwhelm the target system by sending a large amount of traffic	Slice resource isolation can be used to mitigate this kind of attacks	[50]–[52]
IoT botnets	Remotely take control over the devices and perform some malfunctions	Create a quarantine slice and move victimized devices into that slice and take necessary actions	[53], [54]
Zero-day attacks	Exploits a serious software security weakness that the vendor or developer unaware of	Identifying the vulnerable devices and move them to a quarantine slice until do necessary updates	[53], [54]
Man-in-The-Middle (MiTM) attacks	Breaches the communication channel to intercept the messages between them	Use slice isolation and strong authentication protocols for allocated slices	[52]
Authentication attacks	Stealing legitimate user identities and credentials. Dictionary attacks and brute force attacks belongs to this category	Using different authentication methods for different slices with proper slice isolation	[35]
Message replay attacks	Spoofs transmitted frames and re-transmits them to act as a legitimate user	Enabling slicing at the device and adding fields like timestamp to data, and provide strong isolation with enhanced authentication mechanisms	[35], [52], [55]
Message modification	Alters the legitimate message by deleting, adding, changing or reordering it	Enabling slicing at the device and hashing data with slice specific keys	[55], [56]
Masquerading	Impersonate an legitimate user and trying to gain unauthorized privileges	Slice isolation in order to minimize unauthorized privileges and using powerful key management and authentication mechanisms	[35], [51], [52], [56]

networks via network slicing. Learning theory schemes such as deep learning and reinforcement learning, support to predict user demands and change the resource allocation of slices dynamically according to the predictions [29].

Moreover, network slicing can be used for the realization of IoT applications in critical situations. Network slicing allows rapid deployment of dedicated network slices with relatively effortless configurations over the public network. Thus, the slicing based approach is cost-effective and faster than deploying whole new networks for each IoT application. In this way, network slicing provides the required dynamicity for IoT applications.

3) Existing Slicing Based Solutions: Improving dynamicity in the 5G network through network slicing is a favoured area among researchers. Two areas of enabling dynamicity in network slicing, i.e., dynamic resource allocation [47], [48] and dynamic slice creations for different applications [49], that finally improve dynamicity of IoT networks have been addressed in existing solutions. Moreover, efficient resource allocation algorithms needs to be formulated to improve dynamicity.

C. Improving Security

Security is a fundamental requirement in IoT systems. Billions of resource-constrained devices in heterogeneous IoT applications are now connected into people's day-to-day lives. Because they share sensitive information or are involved in safety-critical operations [57], attackers tend to move towards IoT applications.

1) Description of the Limitation: Most of the IoT devices are resource constraints in design. Thus, it is difficult to implement security solutions on IoT devices. Device vendors tend to use common credentials for IoT devices and most of device consumers do not care to change these default credentials. This increases the vulnerability of the IoT devices to dictionary attacks, while being used by consumers [58]. This will help adversaries gain control of the IoT devices. Such potential reasons may result in a series of different types of attacks in IoT, such as Distributed Denial of Services (DDoS), Man In The Middle (MITM), Zero-day, IoT botnets and ransomware [59]–[62]. Network-level security solutions are vital requisites to mitigate these attacks. Security requirements are diverse in various IoT applications. For instance, security requirements in smart healthcare applications are completely different from that of a smart grid scenario. Therefore, different IoT security mechanisms are needed to fulfill these diverse security requirements [63] of each IoT application in a telecommunication network.

2) Benefits of Using Network Slicing: Network slicing can be used to implement various security solutions for the plethora of IoT applications. Slice isolation facilitates reducing the impact of the security attacks, as well as protecting sensitive information collected via IoT devices. Dynamic deployment of security NFs in the slices allows to tackle the attacks in run-time, without affecting other IoT applications. The ability to create quarantine slices to isolate devices that have suspicious behaviours facilitates to operate those devices under tighter restrictions, until taking necessary actions. In this way, network slicing can be beneficial in improving security of IoT applications. Table III summarises the possible attacks in the IoT applications, along with the possible solutions that can be provided via network slicing to mitigate those.

3) Existing Slicing Based Solutions: According to the existing research work, network slicing is identified as a way of improving security of 5G IoT applications. In [50] and [64], they have proposed methods to mitigate IoT based DDoS attacks through slice isolation and edge computing respectively. While secure keying scheme for network slicing was presented in [56], service-oriented authentication framework was presented in [35]. However, new scientific investigations have to be conducted in mitigating other types of security attacks by using network slicing.

D. Improving Privacy

Along with the expansion of IoT systems worldwide, the necessity of schemes for protecting the privacy of exchanged IoT data has increased. Preserving data privacy plays an ever-increasing role in the IoT applications, which collect sensitive measurements [65].

TABLE IV
KEY IoT PRIVACY ISSUES

Privacy issue	Description	Support from NS	Related works
E2E data confidentiality	Flowed data can be visible to unauthorized third parties	Allocating a separate slice for applications with strong slice isolation mechanisms & use encryption mechanisms in each slice	[52]
Lost of data ownership	Ownership of the data sent by the IoT devices, can be ambiguous	Use different powerful authentication and key management mechanisms within slices	[56]
Bylaw conflict	Location specific privacy schemes should be followed while transmitting data	Changing the configurations in the slices such as VNF arrangement to preserve bylaws within each area	
Different trust objectives	Different IoT applications need different levels of security and privacy requirements	Allocating dedicated slices with different privacy preserving NFs	
Trans-border data flow	Since different countries or regions have different data protection schemes, when transmitting those schemes should be preserved	Allocating different slices for applications with multi-domain slicing	

TABLE V
QoS REQUIREMENTS OF DIFFERENT IoT APPLICATIONS

IoT application	Example services	QCI	Resource Type	Priority	Packet Delay Budget	Packet Error Loss Rate
Smart Transportation	Critical V2X messages	75	GBR	2.5	50ms	10^{-2}
	Noncritical V2X messages	79	non-GBR	6.5	50ms	10^{-2}
Industrial Automation	M2M messages	83	GBR	2.2	10ms	10^{-4}
Smart home & city	eMBB services	80	non-GBR	6.8	10ms	10^{-6}
	Intelligent transport systems	84	GBR	2.4	30ms	10^{-5}
Smart healthcare	Remote surgeries	69	non-GBR	5.5	60ms	10^{-6}
	Tele-medicine	2	GBR	6.8	150ms	10^{-3}
Smart Energy	Electricity distribution	85	GBR	2.1	5ms	10^{-5}
Military applications	mission-critical data	70	non-GBR	5.5	200ms	10^{-6}
AR/VR/Gaming	Real-time gaming	4	GBR	5	300ms	10-6
	AR	80	non-GBR	6.8	10ms	10^{-6}
UAVs & drones	Video (live streaming)	7	non-GBR	7	100ms	10^{-3}
	Control signals	69	non-GBR	0.5	60ms	10^{-6}
Smart Farming	Sensor data transmission	9	non-GBR	9	300ms	10^{-6}

1) Description of the Limitation: The worldwide spreading of IoT devices results in the need for transmitting collected data to remote data centres that requires to be further processed. This has to follow several data privacy standards and regulations, which may be international or specialised for a particular geographical region, such as General Data Protection Regulation (GDPR) [66]. Implementing this diverse set of standards and regulations, corresponding to the geographical specifications is a vital requirement. Privacy requirements are drastically difference in different IoT applications. For instance, the privacy requirements in a smart healthcare application are crucial than the requirements in an environmental monitoring application. Facilitating such diverse privacy requirements of IoT applications over traditional telecommunication networks is a burdensome task.

2) Benefits of Using Network Slicing: Allocation of separate slices with proper slice isolation mechanisms for each IoT application, along with required privacy-preserving network functions, helps to satisfy the diverse privacy requirements of IoT applications. Robust authentication mechanisms and strong slice isolation techniques deny the access to a particular slice from other slices to protect the confidentiality of the IoT application data. The ability to changing the VNF structure of the slices dynamically enhances the difficulty of breaking privacy preserving mechanisms. In this way, network slicing can improve the privacy of IoT applications. Table [IV] describes the privacy issues in different IoT scenarios, along with possible solutions that can be provided through network slicing for ensuring privacy.

3) Existing Slicing Based Solutions: Network slicing can be used to ensure the privacy of IoT applications, but scientific investigations that are directly addressing this area are quite limited. Moreover, some of the existing work can be further extended. An IoT user case-specific privacy-preserving communication scheme presented in [67] can be extended to general applications. In [35], Ni *et al.* proposed an efficient and secure service-oriented authentication framework supporting network slicing 5G-enabled IoT services.

E. Improving Quality of Service (QoS)

QoS can be defined as a form of traffic control mechanism that guarantees the ability to run high-priority applications and traffic under limited network capacity. The measurements of concern in QoS are bandwidth (throughput), delay (latency), jitter (variance in latency) and error rate. Different combinations of these properties are essential in increasing the quality of IoT applications.

1) Description of the Limitation: The IoT has proliferated within massive application areas that need diverse QoS requirements for their optimal behavior. As an example, QoS requirements in autonomous vehicle applications, such as very low latency and ultra-reliability, are completely different from the requirements in environmental monitoring applications. Facilitating all these heterogeneous QoS requirements of different IoT applications through the same infrastructure entails a revolutionising re-engineering of the network architecture [68]. Even in congestion situations, QoS control allows us to fulfill sufficient service quality requirements of the IoT applications with high priority classification. Table V illustrates the requirement of different QoS for different IoT applications [69].

2) Benefits of Using Network Slicing: Network slicing ensures facilitating QoS requirements of different IoT applications, through allocating dedicated slices for each use case. Dynamic resource allocation between slices allows us to accomplish QoS requirements in congestion situations [70].

3) Existing Slicing Based Solutions: Based on the existing related works, QoS requirements of different IoT applications can be facilitated through network slicing. In [68], Yousaf *et al.* presented an architecture to provide QoS requirements of the slices. In [71], Höyhtyä *et al.* used network slicing as an enabling technology in providing QoS requirements in critical scenarios over the public networks. Automated slice resource allocation frameworks can be utilized to maintain the QoS level of highly dynamic IoT applications.

F. Providing End-to-End Orchestration

Whenever a service enabled in a network, the life time of that service has to be managed for proper operation. The service End-to-End orchestrator is responsible for provision, management and optimization of resources for that particular network service.

1) Description of the Limitation: Rapid expansion of IoT within a plethora of applications, increases the number of tenants and different stakeholders who involve in managing the ecosystem. As an example, in a smart transportation application, road authorities, manufacturing companies, maintenance teams, need to cooperate for the well-being of the application. Cooperation these multiple parties is a challenging task. With the augmentation of IoT services, the amount of control channel data related to IoT flown through the network increases. Hence, a proper mechanism is required to mitigate the challenge of managing the amount of IoT control data.

2) Benefits of Using Network Slicing: Network slicing provides a solution for this matter through reducing the network complexity, by dividing the network into small manageable parts. It supports a wide range of customers' and operators' requirements by allowing them to execute required configuration changes at run time to their slices [72]. Increased operational complexity due to a large number of created customised networks can be resolved by an end-to-end network slice orchestrator. The IoT world can be envisioned as the most suitable exploitation for a self-managed and isolated slice of network resources [73].

3) Existing Slicing Based Solutions: E2E orchestration of divergent applications is identified as a critical requirement in modern networks and have been proposed several architectures facilitating this requirement. Network slicing management and orchestration architectures [72], [74] and such an architecture with federated slicing [75] were proposed to serve this requirement. Slice orchestration over multi-domains is discussed as a novel scope in E2E orchestration and it can be further investigated.

G. Better Resource Allocation and Prioritization

IoT networks uses several types of network resources such as computing, storage and networking resources. It is required the allocate these resource efficiently to optimized the resource utilization.

1) Description of the Limitation: IoT networks are consists billions of connected devices which support different use cases with heterogeneous network requirements. The allocation of physical network resources for such vast amount of IoT devices is a complex task. Specially, the dynamic nature of IoT services will leads to constant fluctuation in resource utilization. Moreover, the amount of available network resources is always limited in SP networks. Thus, it is essential to manage these limited resources efficiently. However, most of the time, SPs struggle to utilise the available resources efficiently. Moreover, some of the mission critical and delay sensitive IoT applications such as autonomous vehicles, robotics and AR applications might need prioritization of allocated resources over other IoT applications [76].

2) Benefits of Using Network Slicing: Network slicing, that implies the allocation of resources [28], can be considered as the optimal technology to satisfy diverse network requirements of 5G IoT applications. The primary idea of network slicing is analogous to the concept of Infrastructure as a Service (IaaS) in cloud computing, that shares computing, storage and networking resources among tenants [27]. Moreover, the challenge of varying nature of amount of required resources for a particular IoT use case can be overcome by dynamic adjustment of allocated resources for each slice via automated slice manager functions [77]. Moreover, network programmability is a basic element of network slicing that allows us to alter the network resource utilisation dynamically among IoT applications. Network slicing allows us to prioritize traffic in two techniques: user/traffic prioritization via simultaneous management of the priority among different slices, and prioritization users belong to same slice [47].

3) Existing Slicing Based Solutions: Network slicing is recognised as a superlative technology for allocating required network resources to miscellaneous applications in current related works. Radio resource allocation frameworks [78], [79] and a hierarchical resource allocation framework [80] for network slicing have been presented for this. Mathematical models for resource allocation between slices were developed in [27]. Since most of the proposed resource allocation algorithms are specific to single domain, E2E resource allocation algorithms can be identified as a possible future research direction in this aspect [27].

IV. Network Slicing Based IoT Applications

IoT has been used in many application domains. These IoT applications can be categorised into four key areas according to their requirements (Figure 6). This section focuses on discussing key use cases/applications of IoT and how network slicing can be used to overcome the challenges in these applications. Table VI describes a concise summary of possible slicing solutions for each IoT application scenarios with required technical aspects.

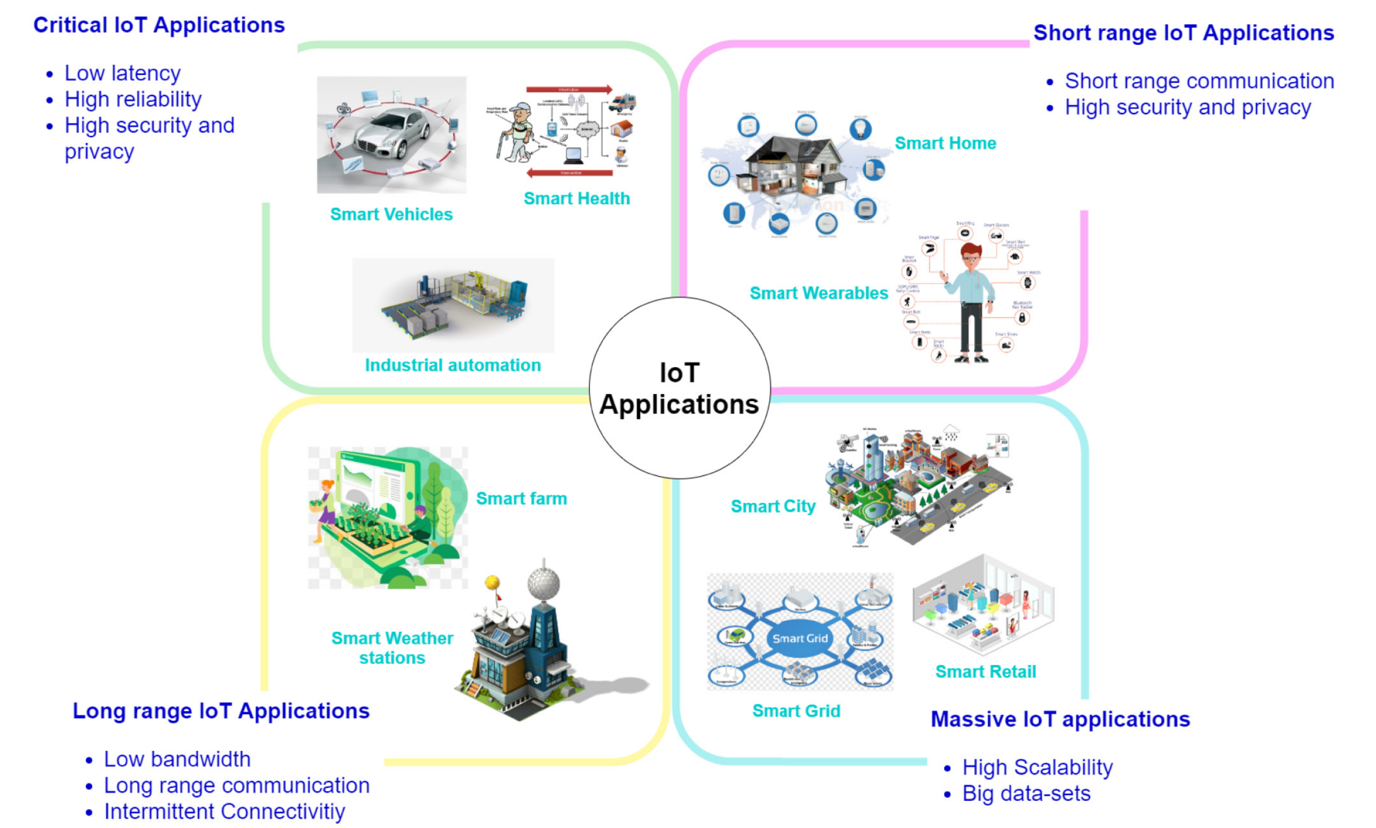

Fig. 6. IoT application scenarios.

A. Smart Transportation

With the mass evolution of the transportation system, IoT has tightly coupled with several areas in transportation, along with vehicle-to-vehicle communication, vehicle-to-infrastructure communication, autonomous or semi-autonomous driving and in-car infotainment systems. Ultrareliability and very low latency are critical communication requirements in Vehicle-to-Everything (V2X) applications [111]. Four different types of communication modes of V2X are identified by 3GPP: vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) and vehicle-to-network (V2N).

1) The Role of Network Slicing in Smart Transportation: V2X covers multiple use cases, such as V2V, V2P, V2I and V2N. Each use case has heterogeneous service and connectivity requirements that cannot be facilitated through a single network infrastructure. Network slicing is the optimal solution to fulfill these requirements in a cost-effective manner. New players such as road authorities, vehicle manufacturers and municipalities that provide multiple services will participate in the V2X scenario, rather than the traditional network provider. It is difficult to support these multiple tenants via infrastructure owned by different operators. A proper set of slice templates can be developed to consummate the requirements of multiple tenants. To manage the high density of moving vehicles, deployment of network functions in the network should be changed dynamically. Also, variations of resource utilisation in network resources by other use cases should not violate

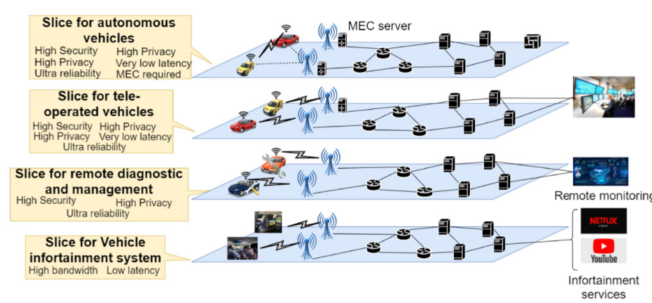

Fig. 7. Network Slicing & Smart Transportation.

the resource requirements of the V2X use cases. Network slicing can provide guaranteed level of network resources for V2X use cases via isolating V2X resources from other application specific slices. Dynamic deployment of network functions according to the time of the day (peak and off-peak) or type of area (rural or urban) increases the efficiency of the network resource utilisation. Moreover, strong security mechanisms can be provided to the communication of different V2X applications through dedicated security network slicing.

Figure 7 shows a brief overview of the network slicing utilisation in smart transportation use case. Four different slices (autonomous vehicles, teleoperated vehicles, remote diagnostic and management and vehicle infotainment systems with diverse network requirements) are depicted here. A slice for autonomous vehicles can be used to facilitate

TABLE VI
ROLE OF SLICING FOR IOT AND ITS PERTINENT DEPLOYMENT CHALLENGES

IoT Application	Slicing based Solution	Advantages of using Slicing									Slicing related Deployment Challenges
		Scalability	Dynamicity	E2E Orchestration	Resource mgt	Recursion	QoS	Adaptive SFC	Security	Privacy	
Smart transportation [81]–[83]	Allocating separate slices for different transportation use cases to provide required network requirements	H	H	M	H	L	H	L	H	H	Large number of third party tenants will be connected to managing transportation and managing them is a challenge
Industrial automation [84]–[86]	Slicing the factory network to facilitate different use cases in a factory environment	L	M	L	L	L	H	L	H	H	Slicing the local factory network and merging the local slices and slices in the public network, are some possible challenges
Smart Healthcare [87]–[89]	Slicing can be used to provide the required QoS requirements, high security and high privacy in healthcare applications	M	M	L	M	L	H	L	H	H	Assuring the security and the privacy of the communicated sensitive information along with required QoS requirements
Smart home and city [90]–[93]	A plethora of applications can be found with slight differences to allocate slices	H	H	M	H	H	H	H	H	H	Security, privacy of these applications as well as dynamic creation and rapid deployment of new slices are challenges in this sector.
AR/VR/Gaming [94]–[96]	Allocating dedicated slices for each AR/VR applications, enables the AR/VR realization within myriad of use cases	L	M	L	M	M	H	L	M	M	Resource management and facilitating QoS requirements are challenges in here
Military applications [97]–[100]	Slicing enables the cost-effective, efficient solution for the realization of military networks on top of public network	M	H	H	H	M	M	H	H	H	Optimal slice isolation with very high security, ultra-reliability and very high privacy are essential in military networks
Smart grid [24], [101]–[103]	Slicing the network facilitates the use cases with diverser requirements in smart grid	H	M	M	M	L	M	L	H	H	Facilitating required QoS with security and privacy in a large geographical area
UAVs and drones [104]–[107]	Dedicated slices with different network properties enables the drone utilization in novel applications	M	M	L	M	M	H	L	M	M	Rapid creation and deployment of new slices with required QoS is a challenge
Farming and environment monitoring [108]–[110]	Dedicated slice with simple network functions facilitate massive number of simple devices	M	L	L	H	L	L	L	L	L	Connecting massive number of simple devices distributed over a large geographical area is a challenging task

H High Impact   M Medium Impact   L Low Impact

communication requirements of self-driving cars. Another slice for teleoperated vehicles can be utilised to manage vehicles remotely in environments that are either dangerous or unfavourable for humans. Communication between car manufacturers or diagnostic centres and vehicles can be facilitated via a slice dedicated for this specific purpose. To provide infotainment services such as Web browsing, HD video streaming and social media access for passengers, a separate slice can be allocated.

2) Related Works: Facilitating communication requirements of smart transportation applications through network slicing have been comprehensively discussed in existing solutions.

In [81], Campolo *et al.* stated that heterogeneous requirements of V2X services cannot be mapped into reference slices in 5G: eMBB, mMTC, URLCC or into a single V2X slice. Besides that, they propose a set of slices for identified V2X use cases that may be consumed by a single vehicle simultaneously: slice for autonomous driving and other safety-critical services, slice supporting teleoperated driving, slice for vehicular infotainment and slice for vehicle remote diagnostic and management. A reference network-slicing architecture for V2X services is proposed in [82], based on a three-layer model [112]: infrastructure layer, service layer, business layer and Management and Orchestration (MANO). In [83], Khan *et al.* have analysed the performance of network slicing in a vehicular network, using a multi-lane highway scenario with two logical slices (the infotainment slice and the autonomous driving slice). They showed that their network slicing approach outperforms the direct Road Side Unit (RSU) method, while attaining high reliability and throughput. Air-Ground Integrated VEhicular Network (AGIVEN) architecture is proposed in [113], to provide high capacity with seamless coverage. The proposed architecture is divided into multiple slices to support a specific application while guaranteeing QoS requirements.

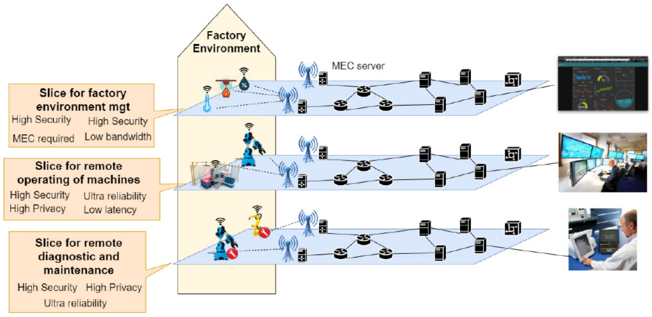

Fig. 8. Network Slicing & Industrial automation.

However, improving security and privacy of V2X network slices and efficient resource allocation algorithms for ensuring network requirements can be further investigated in transportation applications.

B. Industrial Automation/ Industrial IoT (IIoT)

Fourth industrial revolution (Industry 4.0) [114], the novel enhancement in the industrial automation systems, introduces modern communication and computation technologies such as cloud computing and IoT to industrial manufacturing systems [115]. As a result, a large number of IoT devices, machines and applications with heterogeneous network requirements will connect with each other through the network for the realisation of industry 4.0 [116]. Utilising connected IoT based machines rather than human labor with remote monitoring and supervision in a production line will increase the efficiency of the system while reducing the cost. Different types of IoT based sensors can be distributed throughout the factory to monitor the environmental conditions and status of the machines for reducing unplanned downtime.

1) The Role of Network Slicing in Industrial Automation: Existing traditional networks are not capable of fulfilling the diverse communication requirements, like high reliability, low latency and high data rates, of Industrial IoT (IIoT) applications. Network slicing is a viable option for supporting the diverse set of network requirements using the same physical network infrastructure cost-effectively. Changing the NFs, in terms of location and structuring of the slices, achieves various combinations of the properties, such as security, mobility, latency and bandwidth. It is possible to allocate a dedicated slice with guaranteed network resources for a particularly large-scale factory line to accomplish their communication requirements.

Possible use of network slices in a factory environment are shown in the Figure 8. Factory environment management, remote operation of the machines and remote diagnostic and maintenance are the probable scenarios that require separate slices. Thousands of sensors and actuators in the factory can be connected together via a dedicated slice, for managing the factory environment effectively. Workers and machines in the factory can be connected together through a separate slice for remote operation. Machine manufacturers or diagnose centres and the machines can be coupled securely through a dedicated slice to optimize the machines maintenance process.

2) Related Works: Several slicing-based implementations can be found in Industrial automation domain. In [84] and [117], Wu *et al.* demonstrated a practical scenario in conditional monitoring to achieve self-organisation and flexibility, with optimal utilisation of network resources in IIoT networks via network slicing. One of the challenges in IIoT networks that they addressed in their demonstration was the requirement of a quickly accessible and self-organising network. Another challenge they addressed was the necessity for a flexible network to achieve diverse QoS requirements from various services, as well as on-demand optimisation of the network efficiency. Results from their demonstration show the usefulness of network slicing in IIoT systems. In [85], Kalør, *et al.* discussed how network slicing can be used to overcome the challenges in traditional telecommunication systems, by introducing programmability and flexibility to IIoT networks. They have used Industry 4.0 use case to show the network slicing usage to achieve a diverse set of requirements. In [86], Theodorou *et al.* presented a cross-domain network slicing solution developed for EU-funded research project VirtuWind, for an industrial wind park scenario. A two-level hierarchical structure had been proposed to management and control of the network resources. The network slicing process also depends on this two-level hierarchical structure. In [118], Baddeley *et al.* proposed initial efforts to create dedicated SDN control slices in IIoT networks. They have demonstrated the task using IETF 6TiSCH tracks.

Moreover, federated slicing and hierarchical slicing can be considered as novel research directions related to network slicing in industrial networks.

C. Smart Healthcare

Similar to the other application areas, IoT is heavily used in the healthcare system under various use cases [119]. Recent advances in IoT are identified as a potential solution to alleviate the pressures on the healthcare systems, such as medical staff shortage and high healthcare costs, while maintaining quality care to patients [120]. Remote surgery is one of the mission-critical IoT healthcare applications that enables patients to get the service of a set of consultants who are in different places around the world. Remote monitoring of elders and patients who needs continuous monitoring, is an IoT application that requires communication services with ultra-reliability and low latency [121], [122]. As with the prodigious development in the robotic field, employment of humanoid robots near elderly people will support them to live independently at home. Wearable IoT devices is becoming popular in multiple remote monitoring scenarios, such as glucose, ECG, blood pressure and heart rate, for the purpose of avoiding preventable deaths [123].

1) The Role of Network Slicing in Smart Healthcare: Heterogeneous communication service requirements in the diverse set of IoT use cases in the modern healthcare system cannot be accomplished through the traditional telecommunication network. Higher data capacity and extremely fast response time, received through novel 5G technologies, support faster and more accurate results needed for

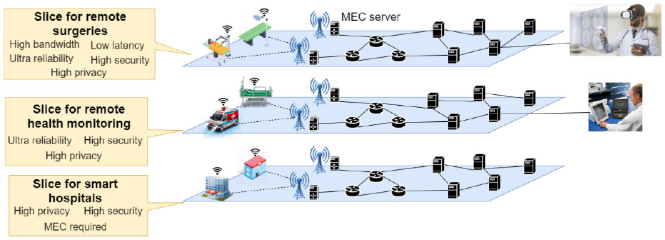

Fig. 9. Network Slicing & Smart Healthcare.

patients' remote monitoring and examination in the healthcare domain [87]. Since the lion's share of the healthcare applications directly deal with the patients' lives, communication services used in the healthcare applications such as remote surgeries should have supreme reliability. While maintaining the promising network resource allocation for these critical healthcare applications, disturbances that will generate through the variation of resource utilisation from other applications should be minimised. Network slicing is the propitious technology that allows achieving this requirement via slice isolation. The ability to allocate resources dynamically to healthcare slices alleviates the resource consumption surges generated through the Internet of Medical Things (IoMT) devices. Security and privacy are primary concerns in the healthcare industry, since it deals with sensitive data of the people. Additional security and privacy can be provided by deploying more security and privacy related network functions in healthcare slices. Slice isolation removes the visibility of healthcare traffic flow to other application slices.

Figure 9 explains how different network slices can be used in the smart health applications. For this sector, separate slices for remote surgeries, remote health monitoring and smart hospitals are identified as required. Applications involving remote surgeries that demand network requirements, such as very high throughput, ultra-reliability and very low latency, can be included into a separate slice. Remote health monitoring applications and wearable devices can be connected to a dedicated slice to provide a secure communication. Medical appliances in a hospital can be networked to a centralised location via a dedicated slice.

2) Related Works: In terms of providing required security, latency and reliability requirements of healthcare-related IoT applications, network slicing is recognised as a dominant solution in existing related works.

In [87], Mavrogiorgou *et al.* proposed a platform to manage healthcare data efficiently with the use of the latest techniques in network slicing, data acquisition and data operability. Through the developed platform, they were able to identify unknown devices and collect their data to assign that into a particular slice to inter-operate with other IoMT devices.

In [88], Celdrán *et al.* proposed an architecture to manage the life cycle of network slicing, while addressing resource orchestration problems, in terms of what, when and how. A policy-based system with two types of policies, intra-slice policies and inter-slice policies, is defined to control the network slices, as well as to change the resource allocation to the slices dynamically. They have thoroughly examined the remote care use case for highlighting the necessity of managing network slices through defining the remote healthcare slice for various requirements of dynamic healthcare environments. In [124], Pries *et al.* demonstrated allocating a network slice for a smart health use case, that connects a smart wearable device with a specific traffic pattern to the cloud efficiently. Innovative eHealth system, powered by 5G network slicing, was proposed in [89]. In there, they have studied the health data collection and analysis from various IoT medical devices via 5G networks. Dynamic provisioning of 5G slices according to the medical devices with diverse requirements was considered in their proposed architecture.

D. Smart Home and City

The smart home concept is extended up to smart offices, smart buildings and finally, to smart cities. Making people's lives smarter through automating day-to-day activities, cost reduction and energy preservation are major advantages of IoT utilisation in smart home and city applications. Smart home applications are ranging from a simple temperature sensing system that automates the functionality of the air conditioner, to an advanced image processing system that identifies intruders, to increase the protection. Despite the advantages of IoT from a smart home perspective, the rate of adoption of IoT devices to their homes by users depends on their desire to buy those devices. Security and convenience have been identified as the key factors that influence their decision [125]. Rapid population growth and urbanisation around cities tend to utilise most of the resources around the earth in a very limited space. This dramatic expansion of cities should be addressed sustainability while increasing the quality of life. The IoT has been made use of to tackle these issues with the smart city concept [91].

1) The Role of Network Slicing in Smart Home and City: Heterogeneity of IoT devices in homes is varied from very primitive devices with very limited energy, to very powerful devices that need a continuous power supply and from insecure devices, to devices with very high-security mechanisms [92]. Since security devices like door locks, surveillance cameras, lights, sirens, smoke detectors and garage door openers deal directly with the security of homes, intruders who take control of those devices are able to create negative effects to the homeowners. Network slicing is a way to eliminate such negative effects to some extent through slice isolation and implementing various security functions in the smart home slice. Smart city applications such as waste-management systems, automated-road-lamp systems, connected-traffic-control systems and smart-parking systems will be connected together to facilitate centralised management. Since a majority of these IoT devices are very simple and use batteries, energy-efficient communication services is a vital requirement with very high security, as it deals directly with the daily living styles of the people who live in the city. Network slicing is the prominent technology to fulfill the communication requirements of such devices. This can be done via allocating a separate slice with lightweight network functions and isolating this traffic stream from other traffic.

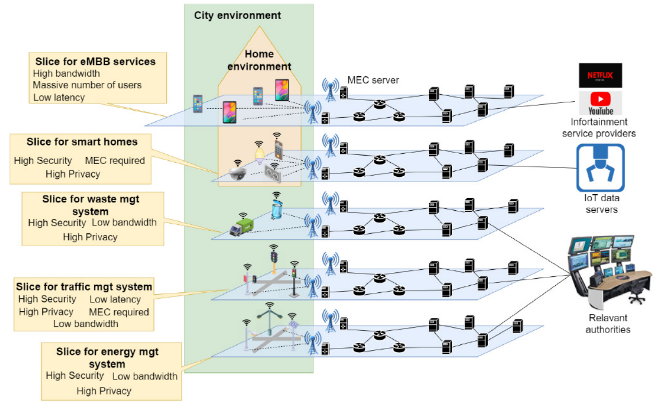

Fig. 10. Network Slicing & Smart City & Home.

Some of the possible network slices with their network capabilities in a smart home and city environment is depicted in Figure 10. Though a large number of slices is realisable in a smart home and city environment, five key scenarios among them are shown in the figure: eMBB services, home management, waste-management system, traffic-management system and energy-management system. Since eMBB devices are distributed over smart homes and smart cities, they can be connected to a single dedicated slice. Smart devices in a home can be connected to a distinct slice to assure secure communication.

2) Related Works: In [92], Dzogovic *et al.* proposed a network slicing-based smart home system, using three different end-to-end slices. Slice dedicated to the home security system, eMBB slice to devices that demand high data rates and massive IoT network slice to provide low-data rates for low-power devices are proposed in the paper. In [93], Chaabnia and Meddeb presented a model for smart home, using network slicing. In their scheme, smart home applications are sliced into four different classes according to their usage, bandwidth requirements and traffic type. In [126], Boussard *et al.* presented an end-to-end research solution, called Future Spaces, based on SDN and NFV, to dynamically control people's digital assets. They have used network slices to provide secure access to devices.

E. AR, VR and Gaming

Augmented Reality (AR), which brings digital elements to live view, and Virtual Reality (VR), which completely replaces the live view with a digital view, are the novel technologies that have the ability to join the physical world and digital world. AR, one of the disruptive technologies developed under the expansion of IoT, is used to improve the interaction between human and computer in a more entertaining manner within smart environments [94]. Mobile phones can be used as AR visors at the early stage, to evaluate the effectiveness of AR in IoT. After this, the transition can be done to multiple alternative options, such as head-mounted displays like Google Glass, Magic Leap Lightwear and Microsoft Hololons, and other wearables that allow users hands-free interaction with IoT services and objects [95]. VR with IoT provides a huge contribution to facilitate indispensable services like remote surgeries, tourism industry, remote meetings, retail, marketing and smart education, as well as entertainment activities. In [96], Alam *et al.* proposed a monitoring and safety system using AR/VR technologies and various IoT devices. Remote monitoring and supervision are possible with the proposed solution. The traditional gaming industry has faced a massive transformation along with AR/VR technologies with IoT devices. It is viable to connect multiple players around the world to the gaming environment and enhance the gaming experience, rather than playing in a isolated environment. A rapid growth of the VR-based gaming market was achieved over the past few years, due to the development of innovative accessories and wearables. The majority of startups who enter the electronic games industry tend to engage with VR technology to develop their games [127].

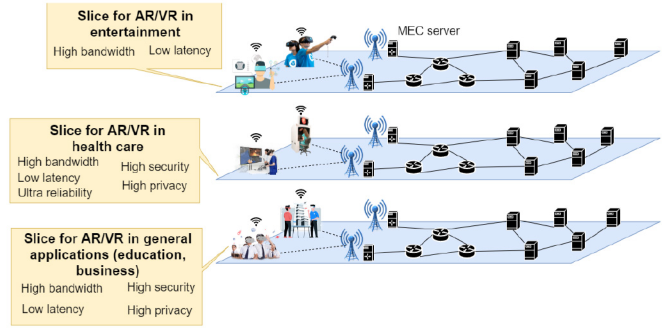

Fig. 11. Network Slicing & AR/VR/Gaming.

1) The Role of Network Slicing in AR, VR, and Gaming: More latency causes experiencing disorientation and dizziness (cyber-sickness) to users while consuming AR/VR devices. Hence, the Motion-To-Photon (MTP) latency is required to keep less than 20ms. Accordingly, considerable range for network-side latency must be 5 to 9ms [128]–[130]. Existing traditional networks are not capable to facilitate this requirement. In the cases of remote surgeries and virtual meetings, security and privacy are critical requirements, since they are directly dealing with the sensitive information of mankind. AR and VR-related applications need very high data rates. For a low resolution, 360 degree AR/VR video requires bandwidth around 25Mbits/s, and according to the quality of the video, the required bandwidth ramps up significantly [128], [129]. These heterogeneous network requirements can be facilitated through network slicing. The standard eMBB service scenario in the novel 5G architecture is designed to facilitate these kinds of applications. Customised network slices can be used to provide specific network characteristics of the AR/VR applications that cannot be facilitated through the standard eMBB slice.

Figure 11 shows the allocation of different network slices in the AR/VR/gaming applications. Since AR/VR entered a plethora of application scenarios, it is feasible to categorise those scenarios within three slices, according to the network requirements as depicted in the figure: slice for AR/VR in entertainment that includes real-time games, slice for AR/VR in healthcare and slice for AR/VR in general applications such as education, business, and tourism.

2) Related Works: In [131], Esteves *et al.* proposed a Proof-of-Concept (PoC) to use the user's location to the placement of a network slice. They considered an interactive-gaming event that has multiple players who access the gaming application simultaneously, in implementing their PoC. A dedicated network slice is used to facilitate the QoS/QoE requirements of the gaming service provider to users. In [132], SK Telecom and Ericsson reported that their ability to create different virtual network slices optimised for AR services.

Since AR/VR is relatively a recent application area, network slicing utilisation is not much covered in existing scientific investigations. However, AR/VR realisation via network slicing has been proved only by some companies through demonstrations [132].

F. Military Applications

IoT integration with technologies, such as wireless sensor networks, embedded systems, M2M communications, cloud computing and mobile applications, has the potential to serve mission-critical military applications. IoT deployment in military applications has primarily focused on battlefield applications. Millions of sensors deployed on multiple applications are used to serve the systems of Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR). The situational awareness gained through those sensors helps senior commanders to steer the battalion and helps warfighters to combat strategically [97]. In [98], Wrona discuss some important use cases for IoT deployment in military applications, such as smart equipment, situational awareness, logistics and medical care. Military IoT (MIoT) supports to realise the concept of "anytime, anyplace connectivity for anything, ubiquitous network with ubiquitous computing" in the military domain. It increases the efficiency of the utilisation of military resources via implementing and managing military diversification affairs more accurately and dynamically [99]. Use of IoT-aided robotics in military applications are discussed in [100] within the following activities: detection of hazardous chemicals and biological weapons, autonomous vehicles in battlefields, support on civil operations in war fields, deactivation of nuclear weapons and access control of people in restricted areas.

1) The Role of Network Slicing in Military Applications: End-to-end secured communication is a crucial requirement in the battlefields for scenarios like communication between soldiers and the control centre and transmission of the information gathered by the IoT devices. Using an existing public network infrastructure with large coverage is a cost-effective solution. Without specifying a separate slice in the physical network with appropriate security functions and strong slice isolation mechanisms, security requirements can't be accomplished. In the applications such as IoT-aided robotics and Unmanned Aerial Vehicles (UAVs), very low latency, ultra-reliability, and high bandwidth are critical network requirements. Traditional telecommunication networks are not capable to facilitate these requirements along with the required security in military use cases. In [71], Höyhtyä *et al.* discuss how to implement critical communication services over a commercial 5G mobile network. They also talked about creating rapidly deployable networks for emergency and tactical operations, using techniques such as network slicing and licensed shared access.

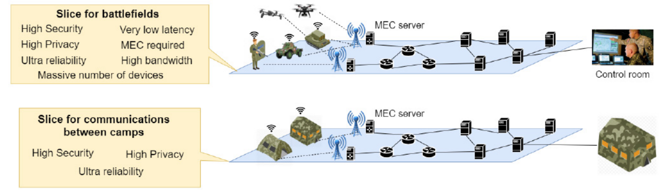

Fig. 12. Network Slicing & Military applications.

Figure 12 explains how network slicing facilitates network requirements in the military IoT. Two important cases for allocating slices have been identified and they are shown in the figure: slice for a battlefield and slice for general defense communication. Fast temporary deployments of slices dedicated to a battlefield can facilitate communication requirements of drones, smart weapons and soldiers. A portion of the public network with high security mechanisms can be permanently allocated to general-defense communications.

2) Related Works: In [133], Grønsund *et al.* discussed the implementation of military communication services over the 5G network via network slicing. They proposed two network slices for military mobile users: military slice for military services which requires more restricted access and security and commercial slice for traditional services. The methodology of providing the basic service requirements of military communications such as isolation, security, high availability, QoS, and performance, via network slicing has been discussed. Moreover, they described the basic implementation of the military slice based on the 5G URLCC slice.

G. Smart Energy

The smart grid can be identified as an electrical system that consists of operations such as electricity generation, transmission, distribution, control and consumption. It uses two-way flows of electricity and information, along with computational and communication technologies to achieve an automated and distributed energy-delivery network, with properties such as clean, safe, secure, efficient, sustainable, reliable and resilient [101]. The overall efficiency of the integrated power grid can be improved by using the IoT to form an interactive real-time network connection between the users and power equipment [102]. All kinds of components such as transformers, breakers, meters and capacitors in the grid can be made intelligible through IoT. It facilitates the advantages such as enhancing customer engagement, optimisation of renewable energy and reducing maintenance costs. In [103], Sarwat *et al.* divide the smart grid into three main logical entities: Functional Entity (FE), Operational Entity (OE) and IoT Entity (IE). The IE entity is responsible for making the smart grid intelligent by constantly sensing accurate measurements from FE and reporting them to OE. A shift into more renewable and distributed energy generation to reduce greenhouse

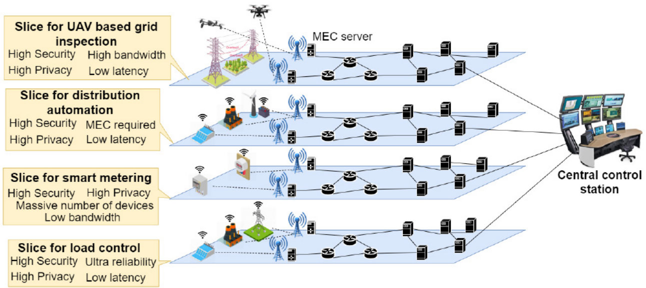

Fig. 13. Network Slicing & Smart Energy.

gas emissions, generates instability in the power grid. IoT helps to remove the instability in the grid through continuous real-time monitoring.

1) The Role of Network Slicing in Smart Energy: Typically, a smart grid consists of a massive number of connected components, distributed across a very large geographical area [103]. These smart components have diverse network requirements [45] across multiple application areas, such as online monitoring for the power transmission line, smart homes and smart vehicles [134]. Some of the complications in the existing network infrastructure include providing a good network connectivity, handling the massive amount of data generated through those components, and facilitating diverse network requirements. Allocation of separate slices for smart grid-based applications in the 5G network can mitigate these complications cost-effectively. The smart grid applications are more attractive to cyber-attacks [135], since a successful attack on a grid can cause a bad impact to the whole country, through creating disturbances in the daily routine of the people, as well as damaging the electric assets. Communication through public networks increases the vulnerability for attacks and proper security mechanisms should be implemented to mitigate these vulnerabilities. Network slicing is a prominent way to implement security functions for grid systems. Slice isolation is a potential solution for segregating the grid-based traffic over the public network.

Different application areas in the smart energy service sector, along with allocating separate slices for each application, are shown in Figure 13. Four different feasible slices have been identified in the smart-grid use case: firstly, for UAV-based-grid inspection, secondly, for distribution automation, thirdly, for smart metering and lastly, for load control. Slices have been allocated according to the network requirements in each use case.

2) Related Works: Allocation of separate slices for identified smart grid applications [24], [136] and increasing the revenue of MNOs through network slicing [137] have been covered in current related works.

In [24], Zhang *et al.* thoroughly examined network slicing in smart grid applications. They have identified four use cases in smart grids, along with different network requirements: Advanced Metering Infrastructure (AMI), Distribution Automation, UAV-based grid Inspection and Millisecond-level precise load control and they proposed separate slices for each use case. The Total Cost of Ownership (TCO) and Return On Investment (ROI) of network slicing in smart grids have been analysed from the operator's perspective. In [137], Dorsch *et al.* discussed the economic advantages that can be achieved through SDN and network slicing when transmitting critical measurements and control commands that required ultra-reliability and low latency in smart grids. They have proposed a techno-economic evaluation approach that consists of smart-grid-traffic modelling, network dimensioning, operator modelling and cost modelling. In [136], Kurtz *et al.* proposed an SDN and NFV based network slicing solution for critical communications in 5G shared infrastructure. They have evaluated the solution using a testing setup for two real-world scenarios - smart grid and Intelligent Transportation System (ITS) - allocating separate slices for each scenario under three cases: performance study, scalability analysis and critical-infrastructure communication. They have achieved higher scalability and low end-to-end delay via their proposed solution.

H. UAVs and Drones

The popularity of Unmanned Aerial Vehicles (UAVs), also known as drones, increased over the past few years in a wide range of areas related to civilian, military, commercial and governmental sectors. Drones have the ability to facilitate multiple IoT services from great heights, forming the airborne IoT through sensors, cameras and GPS modules fixed into drones and emerging telecommunication technologies such as 5G [104]. Surveillance scenarios (e.g., traffic, power line, agriculture and environment) are one of the key aspects in IoT. UAVs can be used to facilitate the requirements of these applications [138], [139]. In [140], Motlagh *et al.* presented an integrative IoT platform operational in the sky, using UAVs equipped with diverse IoT devices. They have implemented UAV-based crowd surveillance applications through the proposed platform. Using drones as aerial base stations is a novel approach in wireless networks to enhance coverage, capacity, energy efficiency and reliability. Attributes of UAVs such as mobility, adaptive altitude and flexibility support some potential applications in wireless systems [105]. This helps to improve the network coverage in remote areas to facilitate remote IoT applications, such as wildlife monitoring and IoT devices that have small transmit power. In addition to supporting IoT applications, UAVs are considered part of the IoT, since their functionality depends on a combination of sensors, antennas and embedded software [106].

1) The Role of Network Slicing and UAVs: There are two main kinds of data that need to be communicated with UAVs, one being control data that needs to handle the UAV. The other is payload data collected from cameras and sensors that needs to be sent to another location for further processing. These data types have diverse network requirements. It needs to facilitate these requirements cost-effectively. High reliability and low latency are key QoS requirements in control data. In payload data, a massive amount of data may need to be transmitted. Along with existing technologies, it is not possible to separate UAV-related traffic from other traffic, as well as control traffic from payload traffic. Network

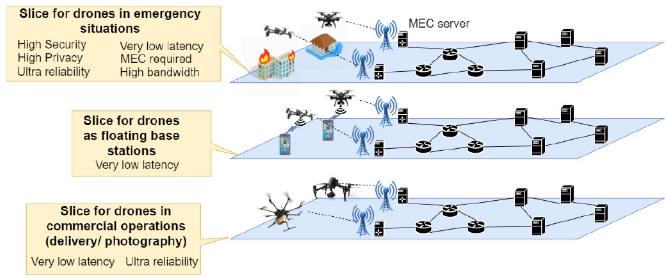

Fig. 14. Network Slicing & Drones.

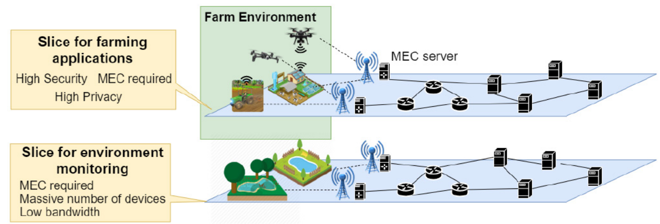

Fig. 15. Network Slicing & Massive IoT.

slicing in 5G networks is a noteworthy technology to facilitate this requirement via slice isolation, while facilitating heterogeneous network requirements in UAV-related traffic.

Figure 14 shows how network slicing can be used in UAV service areas with diverse network requirements. Three possible use cases of drones that required separate slices are shown in the figure: UAVs in emergency situations, UAVs as floating base stations and UAVs in commercial activities like delivery services and photography. Each drone use case can be further sliced to communicate control signals and payload data respectively.

2) Related Works: Accomplishing communication requirements of UAVs and drones, in terms of controlling and other operations such as video streaming, through dedicated network slices, is discussed in current related works. Further investigations should be conducted in the realisation of other UAV use cases, such as aerial base stations and military operations, through network slicing.

In [107], Garcia *et al.* discussed the performance impact of using network slicing in aerial vehicle communications. They have allocated separate network slices to control data and payload data, referred to as control slice and payload slice. The experiment has been done under three trials. In the first trial, they have measured Ipref values in control slice and payload slice in Down Link (DL). The second trial had the same principle with Up Link (UP) and DL. In the final trial, they have checked whether the delay of the control slice is affected by the payload use of the network. They have shown that required throughput of the control slice can be maintained while allocating remaining capacity to payload slice during the flight, via first and second trials. Using the results in the third trial, they have shown that the Round Trip Time (RTT) of control slice is not influenced by the varied payload throughput. They have concluded that slicing performs effectively in facilitating network resources for control communication in aerial vehicle communications. Reference [141] demonstrated how 5G, along with network slicing, can be used in disaster and emergency situations using drones. The demo is executed under two scenarios (delivering supplies and video streaming) in given situations and a dedicated slice is used to provide network connectivity to the drone with required QoS requirements. They have shown how networks can be deployed in disaster situations using network slicing.

I. Massive IoT (Farming, Agriculture and Environment)

The concept of Massive IoT lies on transmitting and consuming a small amount of data from a massive number of IoT devices. Agriculture and environment-monitoring applications are an example for such context, where scale becomes the critical factor, rather than speed [142]. Traditional farms that used to be small units distributed over small land areas have now evolved into massive farms that have thousands of animals over large geographic areas, armed with heterogeneous sensors and actuators. These highly accurate embedded sensors enable precision agriculture by measuring the environmental context inside farms [143], [144]. Improving productivity and maximising yields and profitability, and reducing the environmental footprint, are resulted by the optimal usage of fertilizers, pesticides and efficient irrigation mechanisms [108]. The smart farming concept that includes real-time data gathering and processing, along with automating necessary actions over farming procedures, is realised by precision agriculture. In [109], Ruan *et al.* divided IoT techniques in agriculture into four categories: controlled equipment farming, livestock breeding, aquaculture and aquaponics and open-field planting. They discussed challenges in exploitation of IoT into agriculture. IoT enables environmental monitoring with an assemblage of connected sensors to monitor environmental parameters such as temperature, humidity, wind speed, gases and pressure. It provides advantages such as maintaining healthy growth of crops and ensuring safe working environments in industries [110].

1) The Role of Network Slicing and Massive IoT: International standard organisations identified the massive IoT as one of the main service areas in the novel 5G architecture, which is referred as mMTTC. Network slicing is a promising technology to facilitate network requirements in massive IoT applications that have billions of low power devices with a small amount of data. Narrow Band (NB) IoT is a kind of network slicing technology in Long Term Evolution (LTE) networks, which runs over the same physical network infrastructure. It is designed to facilitate low-cost devices, high coverage, long device battery life and massive capacity [145]. Power consumption of the IoT devices can be optimised via allocating a separate E2E network slice with optimised NFs. Normally, in smart farming and environmental monitoring applications, IoT devices will be distributed in rural areas that do not have a proper network coverage. These devices connect to the network intermittently to transmit collected information, in order to optimise the battery life. Just like NB-IoT, allocating a separate slice facilitates network requirements of these devices over common infrastructure with cost optimisation.

Two application areas, farming and environmental monitoring, in massive IoT are shown in Figure 15 and it describes how network slicing can be used to facilitate network requirements of those applications. Furthermore, dedicated slices with different NFs can be created to other massive IoT applications.

2) Related Works: In [146], Popovski *et al.* discussed heterogeneous non-orthogonal sharing (H-NOMA) of RAN resources in uplink communications of a set of eMBB, mMTC and URLLC devices, which connects to a common base station in RAN slicing. They have analysed slicing of resources between eMBB and URLCC and between eMBB and mMTC, with illustrations of tradeoffs between H-OMA and H-NOMA. In both cases, they have shown that non-orthogonal solutions must be guided by reliability diversity to achieve more efficiency.

J. Other Applications

In addition to the discussed IoT application areas, there are several other applications that can lay hold of network slicing for their realisation. Typically, these applications have less impact from network slicing rather than discussed applications, but have specific advantages.

Smart retail is an application that IoT has dominated in many segments, including supply-chain management, smart vending machines and digital signage. Smart retail is identified as the second-largest MEC use case [147]. Technologies such as AR/VR that require network slicing for its realisation have the ability to influence the customer's decision, finally impacting smart retail [148]. The smart wearable is another application domain that is comprised with several discussed applications, such as smart healthcare, smart city and AR/VR/gaming. Networking slicing with MEC is recognised as a solution to overcome the critical concerns in wearable communications, such as short battery life and limited computing capability [149], [150]. Smart supply chain is listed in the top ten IoT applications in [151]. Tracking goods while they are on the roads and exchanging inventory information, are some possible use cases in the smart supply chain that can be facilitated through mMTC slice over 5G networks.

Table VII summarises the potential network slices and the technical requirements of each proposed slice in each discussed IoT application.

V. Technical Challenges Related to Network Slicing in IoT Realization

This section is allocated to describe the technical challenges related to the network slicing, due to the IoT realisation. The state of the art of each challenge in network slicing will be discussed in detail here.

A. Scalability

1) Requirements: Along with the exponentially rising number of different IoT applications, the number of slices in the network will also increase. Furthermore, service area of a network slice that offer critical services with ultra-low latency requirements will also shrink due to high number of IoT devices. This might finally increase the required number of slices, thus increasing the slice orchestration requests [169]. Thus, the network slice management function should scale correspondingly to mitigate management and orchestration difficulties evolved through the massive number of slices due to the rapid expansion of IoT.

2) Existing Solutions: In [170], Kukliński and Tomaszewski proposed a scalable approach to mitigate difficulties (i.e., massive increment in the number of network slices and involvement of third parties to have slices for their needs) in network slicing management and orchestration. They have introduced a concept called DASMO (Distributed and Autonomic Slice Management and Orchestration), which reduces the management delays and management related traffic, along with enabling the formation of distributed and automated network slicing management solutions. However, the proposed solution is only conceptual and not implemented. In [169], Afolabi *et al.* proposed a novel E2E Network Slicing Orchestration System (NSOS) and a Dynamic Auto-Scaling Algorithm (DASA) for it. Their auto-scaling algorithm scales the resources of their proposed multi-domain orchestration system by handling the large number of slice creation requests to maintain system-wide stability.

Furthermore, efficient algorithms for resource sharing can be investigated to improve the scalability of network slices.

B. Recursion

The ability to create larger functional blocks by aggregating multiple numbers of smaller functional blocks can be defined as recursion [171]. Applying recursion property in network slicing means the creation of new network slices using existing slices [172]. In other terms, network slicing recursion can be defined as methods for network slice segmentation, allowing a slicing hierarchy with parent-child relationships [173].

1) Requirements: IoT applications can span across multiple tenets and network domains. Therefore, creation a completely new slice is a complex task when comparing with using existing slices. Due the dynamicity of IoT use cases, the creation of new slices is a frequent operation which has to accommodate in many networks. Most of the time, there is no be significant differences between the use cases and hence the characteristics of the requested slices. Therefore, it is beneficial for most of the IoT applications to create new slices by inheriting properties from parent slices. This will optimise the slice creation operation in IoT context.

2) Existing Solutions: In [174], Héno *et al.* presented a recursive network slicing model. The proposed model is based on a parallel analysis between IT virtualisation and network virtualisation, using virtualisation theory introduced by Popek and Goldberg. Isolation, recursiveness and independence are considered in their model. They showed how to enable new Business-to-Business-to-Consumer (B2B2C) business models through network slicing by re-renting rented resources achieved by recursive building of network slices layered and nested within each other.

C. Adaptive Service Function Chaining

The network softwarization concepts, especially NFV proposed to used virtualized network functions or services than hardware based network services such as firewalls, Network

TABLE VII
SUMMARY OF EXPECTED PERFORMANCE IN THE IOT APPLICATIONS WITH POSSIBLE SLICES

Use-case	**Slices**	**Expected Scalability**	**Expected latency**	**Expected Bandwidth**	**Type of data support**	**Data Capacity**	**Existing Implementations**
Smart transportation [152], [153]	Autonomous vehicles	50-200 per vehicle	1ms	10 Mb/s (downlink/downlink)	stream/real time	$\geq$ 100 GB per vehicle per day	[81]
	Tele-operated vehicles	50-100 per vehicle	20ms	25 Mb/s for video and sensors data (uplink), 1 Mb/s for application-related control and command (downlink)	stream / real time	$\geq$ 100 GB per vehicle per day	
	Remote diagnostic	10-20 per vehicle	not a concern	not a concern	historical data	not a concern	
	Vehicle infotainment system	5-15 per vehicle	100ms	0.5 Mb/s (web browsing), up to 15 Mb/s for UHD video streaming	stream	$\geq$ 10 GB per vehicle per day	
Industrial automation [154], [155]	Factory env mgt	1 million per factory	$\leq$10ms	10 Mb/s (downlink/downlink)	stream / massive data	80,000 GB per day	
	Remote operating machines	10000 per factory	$\leq$1ms	10 Mbps to 1Gbps	stream/real time	20,000 GB per day	
	Remote diagnostic & maintenance	10000-20000 per factory	not a concern	not a concern	historical data	not a concern	
Smart Healthcare [156]–[159]	Remote surgeries	10-100 per surgery	$\leq$ 200ms	137 Mbps - 1.6Gbps	stream/real-time	1.5 million per year	
	Remote health monitoring	1-10 per consultancy	$\leq$ 1s	10 Mbps	Stream/real-time	1 GB per patient per study	
	Smart hospitals	10-15 devices per bed	$\leq$ 1s	100 Mbps	stream/real-time	10Gb per bed per day	
Smart home & city [160]–[162]	eMBB services	$\geq$ 2000 units/km^2	UP - 4ms, CP - 20ms	DL 100 Mbps, UL 50 Mbps	Stream/real-time/historical	$\geq$ 1,000 GB per day	[92]
	Smart home	10-100 per house	1 ms -1000 s	5Mb/s	realtime	10 MB per home per day	
	Waste management	$\geq$ 50 units/km^2	$\leq$ 1 day	$\leq$ 100KB/s	historical data	20-100 packets per device per day	
	Traffic management	$\geq$1000 units/km^2	$\leq$ 1s	$\leq$ 1 Mb/s	real-time data	$\leq$ 1Gb per unit per day	
	Energy management	$\geq$500 units/km^2	$\leq$ 10 min	not a concern	real-time data	$\leq$ 10Mb per unit per day	
AR/VR/Gaming [163]	Entertainment	$\leq$ 1 billion globally	1ms	25Mbit/s	stream/real-time	$\leq$ 1Gbps	
	Healthcare	10-100 per surgery	$\leq$ 200ms	137 Mbps - 1.6Gbps	stream/real-time	1.5 million per year	
	General applications	$\leq$ 1 billion globally	1ms	25Mbit/s	stream/real-time	$\leq$ 1Gbps	
Smart energy [164]–[166]	Grid inspection	not a concern	1ms -10 ms	$\geq$ 45Mbps	stream/real-time	not a concern	[24], [165]
	Distribution automation	$\geq$ 0.5 billion per grid	$\leq$ 15ms	100Mbps	stream/real-time	$\geq$ 50,000 GB per day	
	Smart metering	$\geq$ 1000 connections/km^2	$\leq$ 1min	1-100 kbps	real-time/historical data	100Mb per day per device	
	Load control	$\geq$ 0.5 billion per grid	$\leq$ 8ms	100Mbps	real-time data	$\geq$ 50,000 GB per day	
UAVs and drones [166], [167]	Emergency situations	not a concern	1ms - 10 ms	$\geq$ 45Mbps	stream/real-time	not a concern	[107]
	Floating base stations	$\geq$ 10 connections/km^2	100ms - 200ms	$\leq$10Mbps	stream/real-time	$\leq$ 1GB per day per UAV	
	Commercial applications	1 million pkg/day	$\leq$ 100ms	$\geq$45Mbps	stream/real-time	$\geq$ 5GB per flight	
Farming and environment monitoring [168]	Smart farming	100-100,000 per farm	1 hour	25Mbps to 1000Mbps	intermittent	$\geq$ 1GB per farm	
	Environment monitoring	$\geq$ 1000 devices/km^2	several hours	$\leq$100kbps	intermittent	$\geq$ 1GB per km^2 per hour	

Address Translation (NAT) and intrusion protection. These vitalized networks services have to execute in certain order to satisfy a particular business need and facilitate the service policy and operational requirements. Linkage of these network functions to form service can be defined as Service Function Chaining (SFC) [175]. Improved operational efficiency and automated handling of traffic flows with advance features (i.e., more security, lower latency or overall high QoS for connected services) can be achieved through SFC [176]. A network slice can be also identified as a collection of connected VNFs. According the nature of supported applications, it is necessary to dynamically change the structure of the slices. This can be realized via by implementing adaptive service function chaining.

1) Requirements: IoT applications are highly dynamic and the network requirements, such as security, latency and QoS are always changing. Using dynamic service chaining, network operators will be able to create, scale, modify and remove network functions of a network slice according to the such changing demand, networks and cloud context information [177]. Recurring changes of network requirements of IoT applications entails continuous updates of SFCs of network slices to reduce the network cost. Hence, adaptive SFC in network slicing is a challenge that has to address due to the evolution of IoT applications.

2) Existing Solutions: In [178], Li *et al.* introduced a novel concept of an elastic service function chain. They addressed network slicing with such chaining constraints as a Software Defined Topology (SDT) (performs slice framing) problem. They formulated the SDT problem (when VF sharing across services, node overlapping may appear between logical topologies) with elastic SFC as a combinatorial optimisation problem. Then they devised a fast multi-stage heuristic algorithm to tackle it.

D. Security

1) Requirements: Several security vulnerabilities can be identified within the network slicing ecosystem. The proliferation of IoT and network slicing exploitation of different IoT applications, intensify the effect of these vulnerabilities. Such issues can be categorized in to three different areas[179].

- Life cycle security aspects for security-related in different phases of the network slice life cycle
- Intra-slice security for security aspects in slice itself and
- Inter-slice security for security aspects between slices

Proper slice isolation is a critical security requirement in network slicing. Since end-device can access more than one slice at once, if there are no strong isolation mechanisms, attackers can launch attacks to other slices relatively easily. Due to the use of lightweight and less complex security mechanisms, IoT devices become attractive for many attackers to perform such attacks.

Involvement of third parties increases due to the IoT expansion. Specially, new set of attackers such as cyber criminals and terrorist will also target IoT application when they are used in Critical National Infrastructures (CNIs). In such scenarios, slice-related configuration and management operations are given to third parties via Application Programming Interfaces (APIs). These APIs are an entry point for intruders to enter and perform unauthorised activities.

2) Existing Solutions: Exploitation of IoT in a plethora of applications increases the security challenges of network slicing and several mechanisms have been proposed to mitigate these challenges.

In [180], Khettab *et al.* proposed and evaluated a novel Security as a Service (SECaaS) architecture that leveraged SDN and NFV to secure a network slice. This ensured an optimal resource allocation that efficiently manages the slice-security strategy. Their proposed architecture consists of four main parts: cloud network, each managed by a Virtual Infrastructure Manager (VIM), VNF managers to monitor a set of VNFs in a slice, an NFV orchestrator responsible for life cycle managing of VNFs and an SDN controller to monitor and control traffic flows. Along with deploying and managing security VNFs (including Intrusion Detection/Prevention System [IDS/IPS] and Deep Packet Inspection [DPI]), the capabilities in their proposed architecture include monitoring their performance and predictive auto-scaling based on pre-defined policies, to ensure the elasticity.

In [65], Cunha *et al.* presented a detailed discussion on security challenges of network slicing at the packet core. Applying AI techniques in achieving security in network slices is discussed in [181]. They have discussed various security challenges with possible AI mechanisms, in order to mitigate those attacks in network slicing. Reference [182] discusses implementation of a quarantine slice to isolate devices that were subjected to a security attack to perform security-related operations for those devices and to minimise the effect of the attack on the other systems.

E. Privacy

1) Requirements: Network slicing has its own set of privacy issues and integration of IoT will further increase the impact of it. Information leakages between slices expose the sensitive data to third parties, endangering the privacy. Strong slice isolation techniques with secure inter-slice communication via secure channels are a critical requirement in using network slicing for communications in order to preserve the privacy of the users. Also, slice isolation mechanisms should be implemented in customer-end devices to assure the privacy of the data from the customer end intruders. Some of the end IoT devices can access more than one slice simultaneously may also be a cause for information leakages between slices.

In [65], Cunha *et al.* discussed the probable security and privacy breaches in network slicing descriptively. Network functions that may be shared between slices are allowing unauthorised inter-slice communication, challenging the confidentiality and the integrity of the data communicated through slices. IoT tenet might ask to use such third party network functions in their slices which might jeopardize the whole slicing system. Successful impersonation of the NSM allows subverting slice isolation, resulting in unauthorised access to all the slices that could be resulted in a breach of system confidentiality and integrity. The ability to change the management and configuration via APIs for third party tenants allows them to impersonate the host platform and run as an authorised platform. By exposing the network and private services to an attacker, confidentiality and the integrity of the system can be endangered. The mentioned privacy issues can become more challenging along with the rapid exploitation of IoT with network slicing.

2) Existing Solutions: Based on the existing solutions, slice isolation [183] and securing inter-slice communication [184], [185] have been identified as solutions to address privacy challenges related to network slicing. Furthermore, investigations can be conducted in preserving privacy in communications when sharing network resources between slices.

In [184], Liu *et al.* proposed two heterogeneous signcryption schemes to accomplish mutual communications between the Public Key Infrastructure (PKI) and the CertificateLess public key Cryptography (CLC) environment, in order to ensure secure communication between network slices. PKI-CLC Heterogeneous Signcryption (PCHS) and CLC-PKI Heterogeneous Signcryption (CPHS) are the proposed schemes in there. They presented how to secure communication between a mobile Internet slice and a vehicle Internet slice using proposed schemes. In [183], Kotulski *et al.* presented a detailed discussion on slice isolation, along with types of isolation, isolation parameters and dynamic slice isolation. These address inter-slice communication to accomplish security perspectives. In [185], Suárez *et al.* presented a mathematical model based on the concept of network slice chains, to manage the inter-slice communication securely when there are different security requirements and attributes between slices. Their proposed model is extensible for application in any service and it complies with any access control model.

F. E2E Management and Orchestration

1) Requirements: The proliferation of the IoT applications increases the need for dedicated slices in the network for their optimal behavior, finally causing the rise of the number of slices that have to be managed. Resource allocation between slices, changing configurations, facilitating QoS requirements and managing the security and privacy aspects for this massive number of slices, are complex tasks that need to be handled efficiently. An abundance of third-party tenants due to IoT collaboration within diverse fields will involve managing and configuring the slices. Managing the involvement of third parties is a challenging task. Temporary usage of slices in emergency situations such as earthquakes, floods and fires make the need for rapid deployment of slices. In addition to the conventional IoT security attacks that are potential to harm telecommunication networks, IoT intensifies the severity of the security threats in the network slicing ecosystem. More robust network slicing management facilities are required to overcome these security challenges. Utilization of a centralised approach for slice orchestration and management will increase the scalability and reliability issues, along with the escalated network slices. According to these facts, IoT systems originate several challenges to the network slice management and orchestration.

2) Existing Solutions: According to the existing solutions, slice management and orchestration can become a complex activity, along with the rapid increment of the number of slices. A couple of MANO frameworks [186], [187] and the MANOaaS concept [188] have been identified as solutions that address this challenge. Future researches can be directed on developing more efficient slice management and orchestration frameworks.

In [186], Meneses *et al.* proposed the SliMANO framework for slice management and orchestration with an implemented and experimentally evaluated prototype. The proposed framework consists of three parts: SliMANO core for coordinating SliMANO functionalities, SliMANO-plugin framework for facilitating the continuous deployment of new plugins and respective agents and SliMANO-agent framework for performing the actions requested by plugins to external network entities. In [188], Yousaf *et al.* shed the light on the concept of MANO-as-a-service (MANOaaS) to customise and distribute the MANO instances between different network tenants for improving the control of network slices. In [187], Abbas *et al.* presented different aspects of slice management for 5G networks. They proposed a framework that exploited Mobile-Central Office Re-Architected as Datacentre (M-CORD) for introducing a slicing mechanism for transport network. It enables slices to be available every time a UE requests them.

G. Other Technical Challenges

Apart from the technical challenges above discussed, a few other technical challenges can be found due to the rise of the IoT realisation. The impact of these challenges is far away from the above-discussed challenges, by reason of lack of large scale network slicing implementations.

Limited nature of the RAN resources such as frequency and time than network resources in the core network such as servers and databases, causes difficulties in RAN slicing. It affects negatively for the E2E implementation and the rapid deployment of the application specific slices. In mobility management and handling roaming scenarios, the same serving slice needs to exist in different operators [189]. IoT devices should be able to cross these boundaries without experiencing any disturbances in communications. Secure and efficient slice information (slice configuration information and user-specific information) transmission between MNOs is required in accomplishing this challenge.

VI. Projects

This section is allocated to discuss some important projects that explicitly work with IoT and network slicing technologies. Most of the projects are based on the Europe region and the recent Horizon 2020 (H2020) funding scheme has fueled for most ongoing projects. Discussed projects along with their technical aspects and the focused research areas, are summarized in the Table IX.

A. SliceNet

SliceNet [191] (1st June 2017 - 31st May 2020) is a project funded by the EU commission under the H2020 program. It aims to develop a management/control framework to support 5G vertical services built as ‘slices’ of network resources. This project drives in achieving three main objectives based on the softwarization of network elements, one being removing the limitations of current network infrastructure. Another is addressing the associated challenges in managing, controlling and orchestrating the new services running in 5G infrastructures and thirdly, maximising the potential of 5G infrastructures and

TABLE VIII
SUMMARY OF RELATED WORKS

Ref	Desc	Application									Technical Aspect								
		Smart Transportation	Industrial Automation	Smart Healthcare	Smart home & city	AR,VR & Gaming	Military applications	Smart Energy	UAVs and drones	massive IoT	Scalability	Dynamicity	Recursion	Adaptive SFC	Security	Privacy	E2E orchestration	Resource Management
[81]	Proposed set of network slices for identified V2X use cases: autonomous driving, tele-operated driving, vehicle infortainment, remote diagnostic and management	✓																✓
[82]	Reference network slicing architecture is proposed for V2X applications based on three layer model	✓																✓
[83]	Analyzed the performance of network slicing in a vehicular network using a multi-lane highway scenario	✓																✓
[113]	AGIVEN architecture with multiple slices is proposed to provide high capacity with seamless coverage	✓										✓						✓
[84]	Demonstrated network slicing as an enabler for flexible and efficient IIoT systems		✓									✓						✓
[117]	Describe how network slicing can be used to practical problems such as surveillance and conditional monitoring in IIoT.		✓										✓		✓			
[85]	Showed how network slicing can be used to mitigate diverse communication requirements in IIoT systems.		✓															
[86]	Described how cross-domain network slicing can be used to IIoT applications with diverse requirements, specialized to wind power plant networks.		✓															✓
[118]	Proposed initial efforts to create dedicated SDN control slices and they have demonstrated the task using IETF 6TiSCH tracks		✓															✓
[87]	Proposed a platform for efficiently manage healthcare data using techniques like data acquisition, network slicing and data interoperability			✓							✓			✓				✓
[88]	Proposed a SDN/NFV enabled architecture to manage the complete life cycle of network slices via dynamically orchestrating the resources with exercising an eHealth use case.			✓								✓					✓	
[92]	Described how network slicing can be used in smart home scenario				✓										✓			✓
[93]	Combined control plane slicing and traffic management on data place by associating data place slicing model in smart homes.				✓													✓
[126]	Used SDN enabled home gateways and VNFs to achieve network security and automation via isolated, usage-oriented slices in smart home networks.				✓										✓	✓		
[131]	Optimization problem tackled through using network slicing to give an idea about latency-aware network slice placement through using a PoC of interactive gaming use case.					✓												✓
[24]	Introduced smart grid use cases and discussed TCO and ROI of network slcing in smart grids to operators							✓							✓			✓

TABLE VIII
(Continued.) SUMMARY OF RELATED WORKS

Ref	Desc	Application									Technical Aspect							
		Smart Transportation	Industrial Automation	Smart Healthcare	Smart home & city	AR,VR & Gaming	Military applications	Smart Energy	UAVs and drones	massive IoT	Scalability	Dynamicity	Recursion	Adaptive SFC	Security	Privacy	E2E orchestration	Resource Management
[137]	Discussed economic advantages that can be achieved through SDN and network slicing in smart grids when transmitting critical measurements and control commands							✓							✓			
[136]	Proposed an SDN and NFV based network slicing solution to critical communications and evaluated it under a smart grid use case.							✓							✓			✓
[107]	Discussed network slicing usage in UAVs and compared effectiveness of slices related to UAV control and UAV payload								✓									✓
[146]	Discussed the coexistence of eMBB, mMTC and URLCC devices within the same RAN network and proposed a resource sharing scheme for RAN								✓									✓
[45]	Argued the way of implementing scalability in the future networks using network slicing		✓								✓							✓
[46]	Discussed a dynamic network slicing concept for allocating resources between fog nodes to improve the scalability							✓			✓	✓						
[170]	Dealt with the scalability problem of management and orchestration problem in network slicing using DASMO concept.										✓							
[47]	Proposed an admission control mechanism to dynamically allocate resources to slices while satisfying users and guaranteeing network requirements	✓									✓	✓						✓
[48]	Dynamic network slicing scheme was proposed for multi-tenant H-CRANs											✓						✓
[49]	Presented an multi-tenant architecture that provide network slices dynamically											✓						✓
[174]	Discussed the methods for recursive building of network slices layered but nested within each other												✓					
[178]	Introduced the concept of elastic service function chaining and addressed network slicing with such chaining constraints													✓				✓
[180]	Proposed an architecture that use NFV and SDN to secure a slice while optimally allocating resources									✓					✓			✓
[50]	Provided a solution to DDoS attacks in 5G network slicing using slice isolation														✓			
[65]	Reviewed challenges of network slicing security														✓			
[181]	Discussed about AI techniques to mitigate security challenges in network slicing.														✓			
[67]	Proposed a privacy preserving communication scheme to smart grid slice	✓						✓							✓	✓		
[35]	Secure service oriented authentication framework was proposed to 5G IoT services supporting network slicing and fog computing	✓								✓					✓	✓		

TABLE IX
CONTRIBUTION OF GLOBAL LEVEL PROJECTS ON NETWORK SLICING AND IoT

		Projects												
		SliceNet [191]	AutoAir [192]	5G!Pagoda [193]	Semantic [194]	Matilda [195]	5G!Drones [196]	MonB5G [197]	5GMobix [198]	Primo-5G [199]	5G-MONARCH [200]	5GCity [201]	INSPIRE-5Gplus [202]	Hexa-X [203]
Technologies	Network slicing	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	IoT	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	SDN	✓		✓		✓					✓	✓		
	NFV	✓		✓		✓					✓	✓	✓	✓
	MEC			✓	✓	✓					✓	✓	✓	✓
Research focus	Network architecture or framework	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓
	Scalability	✓		✓										✓
	Dynamicity					✓						✓		
	E2E orchestration				✓	✓		✓			✓			✓
	Security							✓			✓	✓	✓	✓
	Privacy											✓	✓	

their services. The SliceNet managed domain consists of five layers, from bottom to top respectively: physical infrastructure, virtual infrastructure, service, control and sliced service. The project is running across three main use cases: 5G smart grid self-healing use case, 5G e-Health-connected ambulance use case and smart-city use case.

B. AutoAir

AutoAir [192] project,led by Airspan, is a unique, accelerated program for 5G technology. This is based on small cells that operate on a 'Neutral Host' basis that uses network slicing for allowing multiple public and private mobile operators to use the same infrastructure. This project uses the mobile infrastructure installed at Millibrook. The launch event was held on 12th February 2019 with a demonstration of providing gigabit access to vehicles.

C. 5G!Pagoda

5G!Pagoda [193] (July 2016 - December 2019) is funded by European Commission's H2020 program. The principal goal of the project is to explore relevant standards and align views on 5G network infrastructure. It uses dynamic creation and management of network slices for various mobile services using federated Japanese and European 5G testbeds. They have presented a demo on IoT services via 5G network slicing technology at the IoT week in Aarhus in 2019. The top network-slicing-related objective in this project is the development of scalable 5G architecture with a scalable network slice management and orchestration framework. The IoT-based objective of this project is to develop emerging 5G applications based on IoT use cases and human communication, that require high scalability and customisation of diverse end-user requirements.

D. SEMANTIC

end-to-end Slicing and data-drivEn autoMAtion of Next-generation cellular neTworks with mobIle edge Clouds (1st January 2020 – 31st December 2023) SEMANTIC [194] is a project funded by H2020-EU.1.3.1 and coordinated by Centre Technologic de Telecomunicacions de Catalunya. In this project, they will create an advanced research and training structure for multi-GHz spectrum communications, MEC-empowered service provisioning and end-to-end network slicing. The goal of this project is training Early Stage Researchers (ESRs) to form highly-trained academic researchers and industry professionals in the mentioned areas. This aims to overcome the technical gaps towards the journey to 5G with the guidance from industry professionals.

E. MATILDA

Matilda [195] (1st June 2017 – 30th November 2019) was funded by H2020-EU.2.1.1, aiming to develop a holistic, innovative 5G framework over sliced programmable infrastructure. This is for design, development and orchestration phases of the 5G-ready applications and the network services. One of the main objectives of this project is facilitating vertical industries by enabling the development, deployment and orchestration of network-aware applications via dynamically created application-aware network slices in the 5G ecosystem. It incorporated technological and business requirements that rose from various parties, such as industry, service providers, application users and the research community. The project consisted of four IoT use cases: 5G emergency infrastructure and services orchestration with SLA enforcement, smart-city intelligent-lighting system, remote control and monitoring of automobile electrical systems and an Industry 4.0 smart factory.

F. 5G!Drones

H2020 research and innovation program funded for 5G!Drones [196] (June 2019 - May 2022) project and it is aiming to trial several UAV use cases distributed over eMBB, URLCC and mMTC service areas in 5G architecture. It is also validating 5G KPIs for such challenging use cases. The objectives of this project are validating 5G KPIs and evaluating and validating the performance of different UAV applications. This project covers four use cases: UAV traffic management, public safety/ saving lives, situation awareness and connectivity during crowded events.

Network slicing is featured as the key component in this project, to run UAV services across the network using the same 5G infrastructure. It demonstrates that each UAV application runs independently without affecting the performance of other applications. The results obtained through this project will be used by the UAV association to make further recommendations.

G. MonB5G

MonB5G [197] (November 2019 - November 2022) was funded by the European Union's Horizon 2020 research and innovation program. It is aiming a novel zero-touch-management and orchestration framework for network slicing, to increase the scalability massively for 5G LTE and beyond. This will leverage distribution of operations, together with AI-based mechanisms. Security and energy efficiency are considered key features in their conceptual, hierarchical, fault-tolerant, data-driven network management system, in order to orchestrate a plethora of parallel network slices specific for diverse services. This project consists of two PoCs: zero-touch network and service management with end-to-end SLAs and AI-assisted policy-driven security monitoring and enforcement. The architecture of this project is about splitting the centralised management system into multiple management subsystems that contain one or more distributed management elements. It has the purpose of distributing intelligence and design making across various components.

H. 5GMOBIX

5GMobix [198] (November 2018 - October 2021) is funded via H2020 program and this project is examining the implications of 5G and its role in future autonomous driving. They will develop and test the functionalities of automated vehicles using 5G technology in various environments, such as city and urban. This will be under several conditions like vehicular traffic and network coverage and service demand, considering social and business aspects. Network slicing will be used to facilitate Corporative, Connected and Automated Mobility (CCAM) trial activities in this project.

I. PRIMO-5G

The goal of the Primo-5G [199] (July 2018 - June 2021) project , funded by H2020 program, is to demonstrate an end-to-end 5G system providing immersive video services for moving objects. The project consists of three objectives, one being demonstrating a 5G system to provide video services to moving objects. The second is developing technologies related to mmWave access and 5G core networks. Finally, the third objective is AI-assisted communications to support objective 1, 5G standardisation and spectrum regulation activities. The main envisaged scenario of this project is the firefighting scenario that is a part of the Public Protection and Disaster Relief (PPDR). Drones with cameras will be used by the crew to get real-time situation awareness of the fire scene prior to when they reach to the location, through AR/VR technologies. Network slicing will be used to provide network services for drones and other moving objects in this project.

J. 5G-MONARCH

5G MObile Network ARCHitecture (5G-MONARCH) [200] (1st July 2017 - 30th June 2019) is a project that was aiming to build a flexible, adaptable and programmable architecture for 5G. Network slicing utilization is the specific technical goal of this project. The project consists of two phases. In phase 1, they designed such an architecture at a conceptual level with three enabling innovations. In phase 2, the addressed architecture was brought into practice. The three enabling innovations in this project are inter-slice control and cross-domain management, experiment-driven optimisation and cloud-enabled protocol stack. The developed architecture deployed in two testbeds: the smart sea port related to vertical industry use case and the tourist city related to media and entertainment use case. Resilience, security and resource elasticity are the functional innovations of the instantiated slices in use cases respectively.

K. 5GCity

5GCity [201] (June 2017 – June 2019) is funded by the H2020 research and innovation program. The vision is designing, developing, deploying and demonstrating a distributed cloud and radio platform for 5G neutral hosts. This project was focused on bringing benefits of smart city infrastructure based on resource sharing and end-to-end virtualisation to 5G neutral hosts. The project targeted three different cities (Barcelona, Bristol and Lucca) under three use cases: media, neutral host and unauthorised-waste-dumping prevention. This was to enable the creation of dynamic E2E slices with virtualised edge and network resources to lease to third-party operators. Under the media use case, they will consider three different scenarios: mobile real-time transmission, UHD video distribution and real-time video acquisition and production in edge. For dumping use case, they would use surveillance cameras to monitor and detect unauthorised dumping.

L. Inspire-5Gplus

INtelligent Security and PervasIve tRust for 5G and Beyond (INSPIRE-5Gplus) [202] (November 2019 - November 2022) which is a Horizon 2020 project, aims to address the cyber-security risks of 5G and beyond networks, and vertical applications, ranging from connected cars to industry 4.0, through an innovative security management concept. The project will improve security in several dimensions including, vision, use cases, integration and management, architecture, models, and assets. Ensuring the expected Security SLAs (SSLAs) and the regulation requirements via a fully automated E2E smart network and security management framework, is another objective of this project.

M. Hexa-X

Hexa-X [203] (January 2021 - June 2023) is the European Commission's 6G flagship initiative project which aims to develop and define the architecture, technologies and vision for next generation 6G wireless networks. The research areas of Hexa-X project is focusing on six key topics, i.e., connected

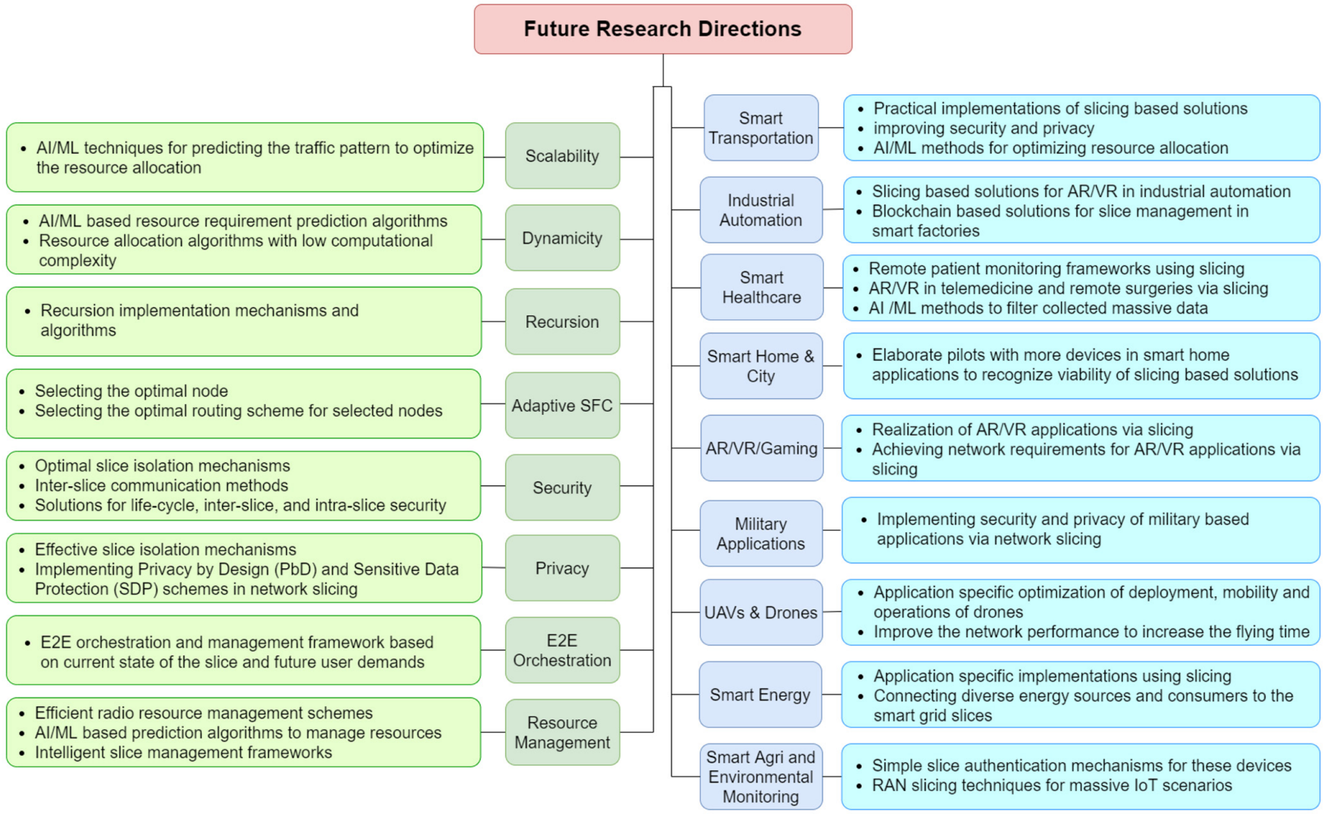

Fig. 16. Future research directions.

intelligence, networks of networks, sustainability, global service coverage, extreme experience, and trustworthiness.

VII. Lessons Learned and Future Directions

This section focuses on the lessons learned and the future research directions with respect to network slicing and IoT integration. Network slicing in different IoT applications, and technical aspects and challenges related to IoT realisation via network slicing will be discussed in here. Figure 16 shows a summary of the discussed future research directions.

A. Smart Transportation

1) Lessons Learned: We explored how IoT can be engaged in different smart transportation applications with diverse network requirements. Autonomous vehicles play a key role in smart transportation. Several pieces of research have been conducted to discuss the realisation of autonomous vehicles, including fulfilling network requirements. We identified that network slicing can be used to facilitate diverse network requirements of different applications in smart transportation. Moreover, MEC helps to fulfill latency requirements in smart transportation applications. Slice isolation is lucrative in implementing security and privacy requirements of transportation communications. Dynamic allocation of network resources with enhanced scalability might be required in slices allocated to transportation due to sudden traffic surges induced from irregular patterns of using vehicles.

2) Future Directions: Though some researches can be found regarding network slicing and smart transportation, most of them are conceptual. Researches with actual slicing implementations can be considered as a valuable movement in the realisation of smart transportation. Since security and privacy are extremely important aspects of autonomous vehicles, the implementation of those aspects using network slicing can be identified as a future research direction. Traffic-prediction algorithms using AI/ML and reinforcement techniques need to be formulated to increase the efficiency of resource allocation between slices, to tackle the traffic surges.

B. Industrial Automation

1) Lessons Learned: Network slicing tackles the generated complexity to the industrial networks. This includes managing and controlling the network, according to the introduced new range of requirements by Industry 4.0. Facilitating the network requirements through allocating resources efficiently via network slicing has been examined in the existing researches. Hierarchical slicing can be used in large scale factories to reduce the complexity in MNO's network and taking the management of the factory network to the factory authority. Utilising network slicing to implement secure industry networks has to be investigated further.

2) Future Directions: Using AR/VR technologies in industrial automation [204], [205] for operating machines remotely is a significant requirement to enhance the performance of a factory line and reduce the cost. Another requirement is remote diagnosing faults and performing necessary maintenance activities in machines. Network slicing is a salient technology that enables this feature and more researches can be conducted in the future in this area. In [206], Backman *et al.*

proposed a novel concept of blockchain slice leasing ledger to autonomously and dynamically acquire the slices needed for increasing the efficiency in future factories. Future researches can be directed in using blockchain technology to the management of 5G network slices that enable several new business models for smart factories, as well as IT infrastructure.

C. Smart Healthcare

1) Lessons Learned: A myriad of use cases of the IoMT [207] intensifies the need of network slicing to facilitate heterogeneous network requirements of each use case. Since IoMT deals with the sensitive information of people, security and privacy of the exchanged healthcare data should be preserved during the communication [208]. Technical aspects in network slicing, such as slice isolation and adaptive SFC to change the security-related VNFs dynamically, are spotted as preserving ways to healthcare data. Network slicing and the 5G network support the realisation of remote surgeries [209] that need ultra-reliable network requirements with very low latency and guaranteed bandwidth.

2) Future Directions: Remote patients' monitoring framework collects valuable information from wearables, heart monitors and infusion pumps to provide better treatment to patients in remote. This is highlighted as a future direction of remote healthcare [88]. Healthcare-data transmission and data-management operations can be identified as very challenging research topics in healthcare [89]. So, the attention of future researches can be paved the way to healthcare-data transmission via network slicing. AI/ML techniques can be used to clean the collected massive healthcare data in MEC servers prior transmitting to the cloud for analysis. Facilitating network requirements in applying AR/VR technologies in remote surgeries and telemedicine via network slicing is an enthralling research direction.

D. Smart City and Home

1) Lessons Learned: Network slicing enhances the efficiency of network resource utilisation, to enable the realisation of a smart city concept that has billions of devices connected together under various use cases. Recursion is discerned as a salient aspect that supports the fast deploying of network slices for homogeneous smart city use cases. Among the smart home diversified-network requirements, security, performance, cost and management shortcomings are addressed via network slicing elaborately.

2) Future Directions: More elaborate pilots with more devices in multiple home applications are required, despite primitive implementations of smart-home solutions. This is to recognise the viability of network slicing in smart homes. Recursive composition of network slices can be researched in order to support smart city use cases.

E. AR/VR/Gaming

1) Lessons Learned: AR/VR is becoming a realisation through the 5G architecture. It extends its roots into multiple service areas including mission-critical scenarios, like healthcare, and entertaining applications, like gaming and movies. Network slicing is recognised as the way of providing the network requirements, such as very low latency and high security required to AR/VR applications over the common infrastructure. Modern games enforced with smart wearables and AR/VR tools that connect people around the world need network slicing to attain its network requirements, such as low latency and high throughput over the public network cost-efficiently. Edge computing [210] is a supported technology for the realisation of the AR/VR.

2) Future Directions: To the best of our knowledge at the time that we are doing the survey, no researches can be found in network slicing and AR/VR applications. Future researches can be directed in the realisation of AR/VR applications using network slicing including satisfying AR/VR network requirements, such as security and high throughput. Implementing the same serving slice within multiple MNOs spread over different geographical regions is required in modern games.

F. Military Applications

1) Lessons Learned: Military applications need extremely secure communication with very high privacy. Network slicing is recognised as the way of enabling secure and privacy-preserved communication in military applications over the public network. Scalability, dynamicity, end-to-end orchestration, recursion, security, adaptive SFC and privacy are all critical requirements in military networks, that can be facilitated through network slicing.

2) Future Directions: As far as we are aware, there are no scientific investigations in this domain. Thus, this area is a novel domain that researchers can direct their researches on the network slicing utilisation in military applications. Since security and privacy are supreme aspects in the defense sector, modern methods for enhancing these aspects are needed. Rapid deployment of new slices for covering battlefields and multi-domain slicing, need to be investigated to facilitate military applications.

G. Smart Grid

1) Lessons Learned: Network slicing is the solution for the realisation of the smart grid that needs several isolated slices for services such as smart metering and UAV-based power-line inspection to facilitate diverse network requirements. Slices need to be distributed over a very large geographical area [211]. MEC can be considered as a viable solution for delay-sensitive applications in smart grids. Higher scalability in the network requested by the massive number of connected devices, such as smart meters to the grid, can be facilitated via network slicing.

2) Future Directions: It is possible to find high-level investigations related to smart grid applications in network slicing. However, scientific investigations specified for a particular application related to the grid are difficult to find and it will open a new research direction. Diverse energy sources and consumers can be connected together to build a more effective smart grid. More researches can be conducted in combining diverse sectors into the grid. Methods to improve the slice coverage are required in smart grid applications.

H. UAVs and Drones

1) Lessons Learned: In addition to the very fast communication requirements for controlling the UAV, high-bandwidth requirements exist for applications like transferring the video recordings collected by the UAV. Network slicing provides these diverse requirements on top of the same physical infrastructure. Slice isolation for providing required resources uninterruptedly is a critical requirement in UAVs, to assure the best functionality.

2) Future Directions: Contribution of Multiple Input Multiple Output (MIMO) systems in UAV communications can be considered as future research directions. Improving the network performance in order to increase the flying time can also be considered. Application-specific optimisation of deployment, mobility and operations of drones [212] are an important research topic that can be tackled using network slicing.

I. Massive IoT

1) Lessons Learned: A massive number of connected devices with low power and low data rates increases the requirement of dedicated network slices with simple network functions over the common network infrastructure, due to simple power-preserving communication requirements. Massive amounts of data collected through the sensors in this application can be processed in the edge to reduce the burden in the core network.

2) Future Directions: Simple authentication mechanisms for these kinds of devices can be implemented as VNFs so that they can be deployed in network slices. They are a vital requirement and further investigations can be done in this area. Scientific investigations related to RAN-slicing techniques for massive IoT scenarios are also an interesting research direction. Methods to improve the coverage of the slices are required when facilitating environmental monitoring.

J. Scalability

1) Lessons Learned: With the exploitation of the IoT for a myriad of applications, an enormous quantity of devices with diverse network requirements exist for connecting. The number of actively connected devices is varying from time to time. This escalates the need for a scalable network. Through slicing the network and changing the network-resource allocation dynamically (with respect to the requirements like the amount of traffic through the slice), network slicing increases the scalability of the network.

2) Future Directions: Extending the proposed dynamic network-slicing framework for fog computing systems into the 5G core network is stated as a future research direction in [46]. Dynamic resource allocation is an important aspect of the operation of improving scalability. The use of prediction algorithms based on the AI/ML techniques to predict the traffic pattern is an enthralling direction that can be used to enhance the scalability of the network.

K. Dynamicity

1) Lessons Learned: Dynamic resource allocation between slices and the ability to deploy network slices dynamically is recognised as two main areas in achieving dynamicity via network slicing. We have identified that the number of active connections and the amount of traffic flowed vary rapidly in the IoT applications. Dynamic resource allocation using network slicing is a possible solution to increase the efficient utilisation of network resources. Rapid deployments of new slices for situations such as disaster management and battlefields, intensify the need of dynamicity of the network.

2) Future Directions: AI/ML-based resource-requirement prediction algorithms are a vital requirement in enhancing the flexibility of dynamic resource allocation between slices and it will be a sophisticated research direction. For efficient dynamic resource allocation, resource-allocation algorithms should be designed with a very low computational complexity [27]. Due to the heterogeneity of Radio Access Technologies (RATs), slicing the RAN is a complex task and it aggravates dynamic RAN resource allocation.

L. Recursion

1) Lessons Learned: Slice creation is a frequent activity due to various slice requirements with slight changes among them. Recursion supports creating slices using the existing slices and it reduces the complexity of creating new slices while fastening the deployment of new ones. We recognised that the recursion supports the rapid expansion of the IoT in novel application areas.

2) Future Directions: Since recursion is a novel concept, there is a lot to investigate under this aspect. To the best of our knowledge at the time we are conducting the research, we couldn't find a dedicated scientific investigation regarding implementing recursion in network slicing. Required algorithms, entities, protocols and interfaces needs to be researched in implementing recursion.

M. Adaptive SFC

1) Lessons Learned: Network slice that is allocated for a particular use case can be identified as an SFC itself. It runs on the principles of SFC [213]. The chain of the NFs will be needed to change according to the different situations, such as deploying a security function when there is a security attack and removing the security function after the attack. The adaptability of the SFC in the network slice supports minimising the cost related to the network in terms of the resources and time, as well as increasing the productivity of the use case.

2) Future Directions: As stated in [29], there are two main challenges in SFC: selecting the optimal node and the routing scheme for the selected nodes. AI/ML-based algorithms can be developed in selecting optimal nodes and the optimum routing scheme for the SFC.

N. Security

1) Lessons Learned: IoT exploitation in critical applications like smart grids and military applications and sensitive applications like smart health, increases the security requirements. To accomplish the different security levels in the IoT applications, network slicing can be considered as one of the optimum technologies. Slice isolation in network slicing is identified as the basic way of providing security between different applications. Deployment of different security functions in the slices is another way to achieve security requirements. In addition to the traditional security challenges, a series of new security challenges have been introduced due to network slicing. Security in network slicing can be divided into three main parts: life cycle security, inter-slice security and intra-slice security [179].

2) Future Directions: Due to the lack of large-scale implementations of network slicing and the ongoing 5G security specifications being prone to change, the analysis of network slicing security is still in an incipient phase [179]. Slice isolation is a critical requirement in achieving security. Several possible research directions can be identified, such as level of isolation and inter-slice communication with slice isolation. As discussed in [179], solutions for life cycle security, inter-slice security and intra-slice security can be investigated. Due to the third-party involvement in management scenarios of network slicing, a series of unknown security attacks will be generated and those can be examined in future researches.

O. Privacy

1) Lessons Learned: Since IoT has entered to the applications that deal with sensitive information like healthcare applications and military applications, privacy became a momentous requirement. Allocating separate slices for different applications with strong slice isolation mechanisms allows privacy-preservation of the data communicated in different slices. The ability to change the privacy-related network functions of the network slice dynamically facilitates to corporate more privacy-preserving facilities into the IoT data streams.

2) Future Directions: As slice isolation is a critical requirement in preserving privacy, implementing an E2E isolated network slice needs to be investigated. Novel privacy-protecting algorithms that can be implemented as VNFs and deployed in a slice can be addressed. Effectuating concepts like Privacy by design and Sensitive Data Protection (SDP) in network slicing to preserve privacy can be studied.

P. End-to-End Orchestration

1) Lessons Learned: Network slicing is an end-to-end technology that enables the deployment of slices, from the customer end to the application backend, through the network. It has the ability to change the configurations in slices according to the SLAs between the tenants and the network providers. This smooths the joining of new applications into the 5G market, including diverse IoT applications. We recognised that the diverse management requirements during the end-to-end traffic flow of various IoT applications can be accomplished using the end-to-end orchestration property of network slicing.

2) Future Directions: Though there are proposed E2E network slicing management and orchestration frameworks, a sophisticated E2E orchestration and management plane is required. It must have adaptive solutions for managing resources holistically and efficiently, through making the decisions according to the current state of the slice, as well as the predictions of future user demands [21].

Q. Resource Management

1) Lessons Learned: IoT increases the resource requirements in the telecommunication networks that can't be satisfied cost-efficiently using traditional methods. We identified that the network slicing is the modern solution for addressing this problem. Assigning a dedicated amount of resources for each slice, along with the ability to dynamically reassign or overbook the allocated resources, increases the resource utilisation efficiency and cost-efficiency of the system [214]. Assuring the SLAs of the connected third-party tenants due to heterogeneous applications, including the IoT, becomes a reality due to network slicing [215].

2) Future Directions: Radio resource management with guaranteeing the diverse QoS requirements is a challenging task [28]. Investigating efficient methods for RAN resource management for RAN slicing is a possible future research direction. In [215], Khodapanah *et al.* highlighted the requirement of an intelligent slice management function for fulfilling the SLAs of different network slices in the network. AI/ML-related algorithms for predicting resource requirements is a novel approach that can be used in resource management in network slicing.

VIII. Emerging and Future Research Directions for Network Slicing and IoT Integration

In this section, we present some of the novel technologies and their impact on network slicing and IoT realisation. Blockchain, AI/ML, multi-domain slicing and hierarchical slicing will be covered in here.

A. Network Slicing and Blockchain

Blockchain is a novel technology that began to attract the attention as the basis of cryptocurrencies such as Bitcoin. It has the ability to vastly improve the existing technology applications, as well as to enable the realisation of the new applications that were never previously practical to be deployed [216]. Blockchain can be identified as a time-stamped series of data that are immutable. This means once data is added to the blockchain, they cannot be deleted or modified. Data is stored in the blocks that are connected to each other and secured, using cryptographic principles. Different kinds of existing blockchain-based activities can be categorised into three areas: Blockchain 1.0 for currency-related operations, Blockchain 2.0 for contracts such as stocks, bonds and loans and Blockchain 3.0 for applications such as health, science and literacy [217], [218]. Blockchain has been rapidly utilised to register, authenticate and validate assets and transactions. It has also been utilised to record data, manage the identification and govern interactions among multiple parties [219]. As well as in the other application areas, blockchains can be utilised in the telecommunication applications such as fraud detection, Identity-as-a-Service and data management, 5G enablement and the IoT connectivity [220]–[222]. In [219], Chaer *et al.* identified the main five areas that can be used blockchain in 5G networks: 5G infrastructure and crowdsourcing, 5G-infrastructure sharing, international roaming, network slicing and management and authentication of mMTC and uRLLC.

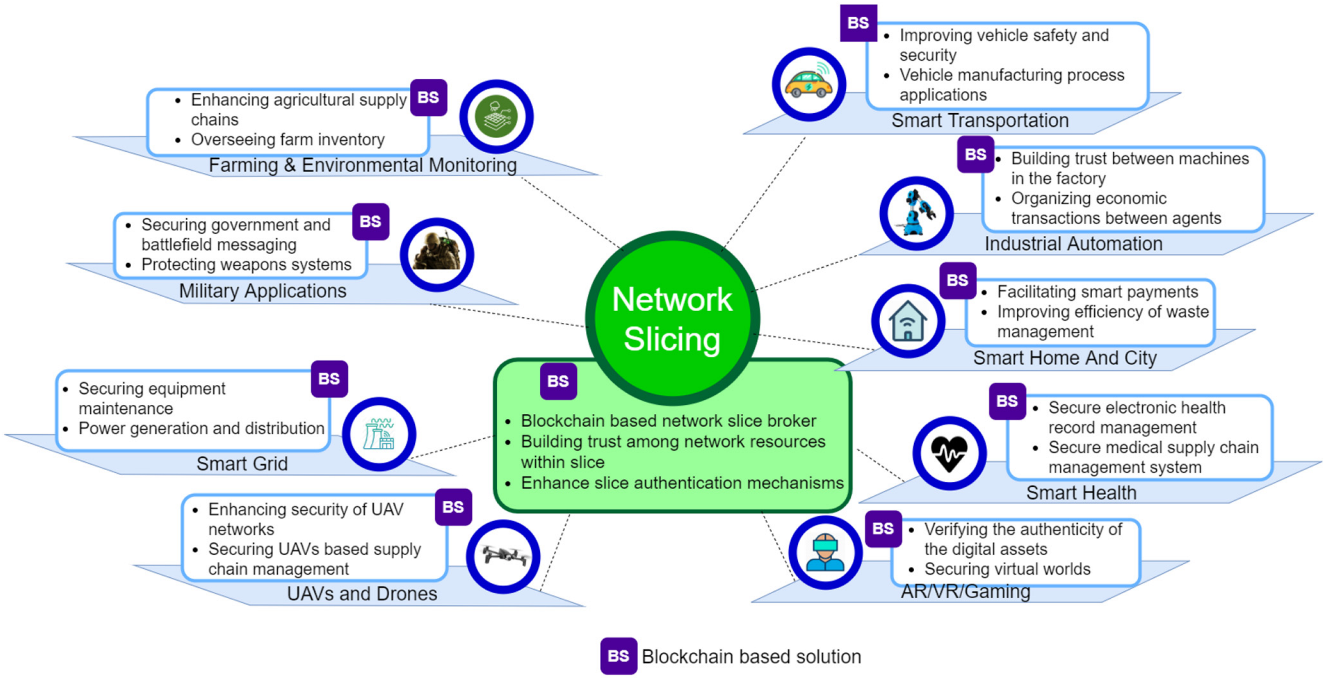

Fig. 17. Role of Blockchain for Network slicing in IoT.

Figure 17 explains how blockchain can be used to achieve benefits in network slicing and in different IoT applications.

Network slice broker is a popular research area of using blockchain in network slicing and several researches can be found in this domain [206], [223]–[225]. In [223], Nour *et al.* proposed a network slice broker design based on blockchain technology. It supports the slice provider that is a new role included in 5G, to select resources from different resource providers and create E2E slices. They envisioned a subslice-deployment-brokering mechanism as a series of small contracts. In [224], Zanzi *et al.* proposed a novel network-slicing-brokering solution that leverages blockchain technology called NSBchain. It allows the allocation of network resources from Infrastructure Providers (InPs) to the Intermediate broker (IB) via smart contracts. It also allows IB to assign and redistribute their resources to tenants in a secure, automated and scalable manner. In [225], Valtanen *et al.* presented a blockchain network-slice-brokering use case value analysis. They used an industrial automation scenario as a use case in their paper that acquired the slices needed autonomously and dynamically.

B. Network Slicing and Machine Learning/Artificial Intelligence

Artificial Intelligence (AI) and Machine Learning (ML) are revolutionary technologies that have become ubiquitous in every field, making machines intelligent in order to make decisions themselves without any human intervention. Telecommunication operators tend to use ML techniques in multifarious areas such as network automation, customer experience, business process automation, infrastructure maintenance and new digital services [226]. ML can be recognised as a necessary part of any 5G network, due to its higher complexity than previous generation networks and the ability to serve a plethora of vertical services including the IoT [227]. Network slicing needs integration and more intelligent capabilities based on ML and big data applications, in order to achieve functionalities such as self-configuration, self-optimisation and fault management [228]. ML techniques (i.e., supervised learning, unsupervised learning and reinforcement learning) have been extensively used in improving network security, including authentication, access control, malware detection and anti-jamming offloading [229]. A comprehensive survey on resource management in cellular and IoT networks using ML techniques, was presented in [230]. Figure 18 shows how AI/ML can be used in network slicing and in different IoT application scenarios.

In [231], Thantharate *et al.* implemented a deep learning neural network, to develop a DeepSlice model to manage network-load efficiency and network availability. It covers three main goals: appropriate slice selection for a device, correct slice prediction and allocating required resources based on the traffic prediction and adaption of slice assignments, in case of network failures. In [232], Mei *et al.* proposed an intelligent network-slicing architecture for V2X services that leverages the recent advancements of ML technologies. A novel deep reinforcement algorithm is proposed to automate the deployment of network slices based on the collected historical data of vehicular networks. A deep reinforcement algorithm was proposed in [233] for resource mapping in 5G network slicing. The proposed RLCO algorithm was able to solve the problems of poor efficiency of existing algorithms in virtual network mapping, low resource utilisation and poor coordination between node mapping and link mapping. In [234], De Bast *et al.* proposed a fast-learning Deep Reinforcement Learning (DRL) model that has the ability to optimise the slice configuration of unplanned Wi-Fi networks dynamically

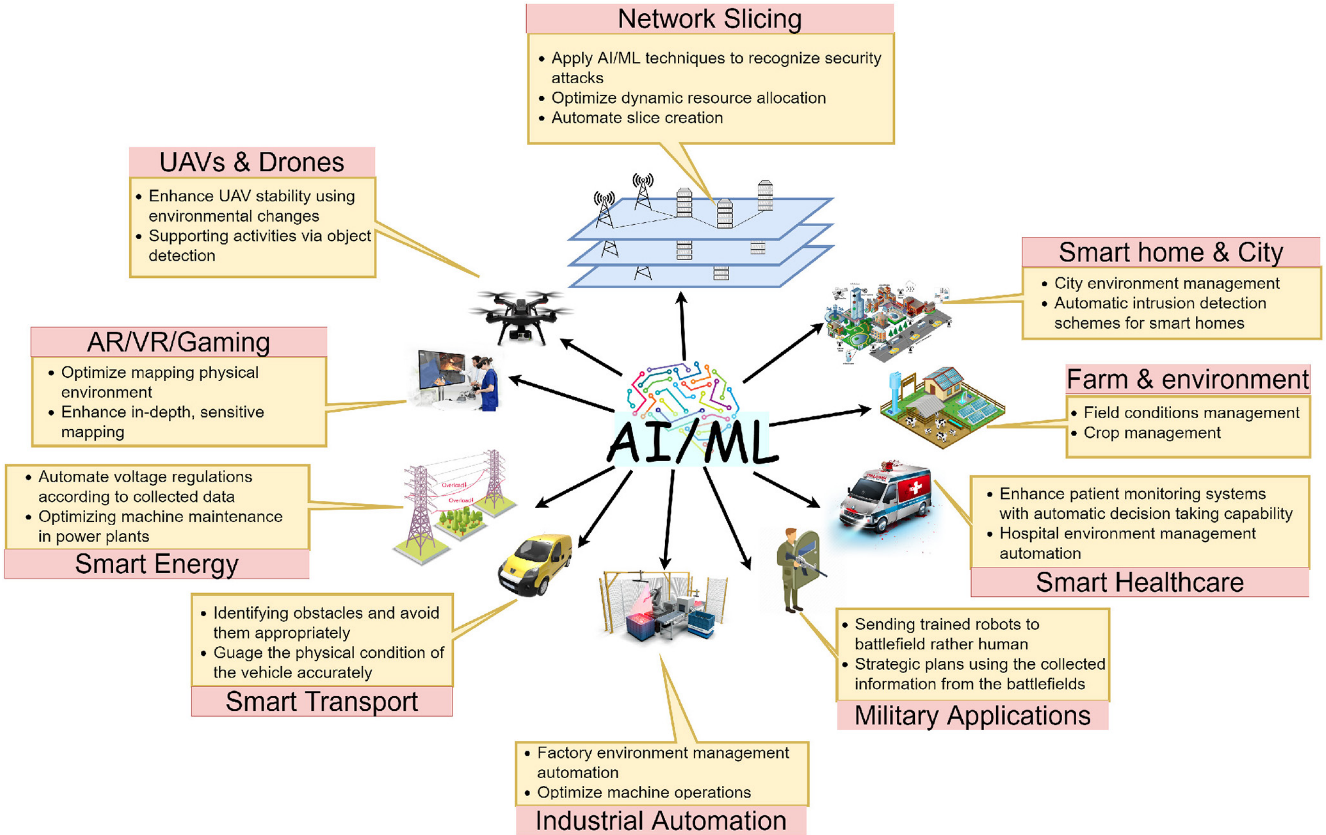

Fig. 18. Role of AI/ML for network slicing in IoT.

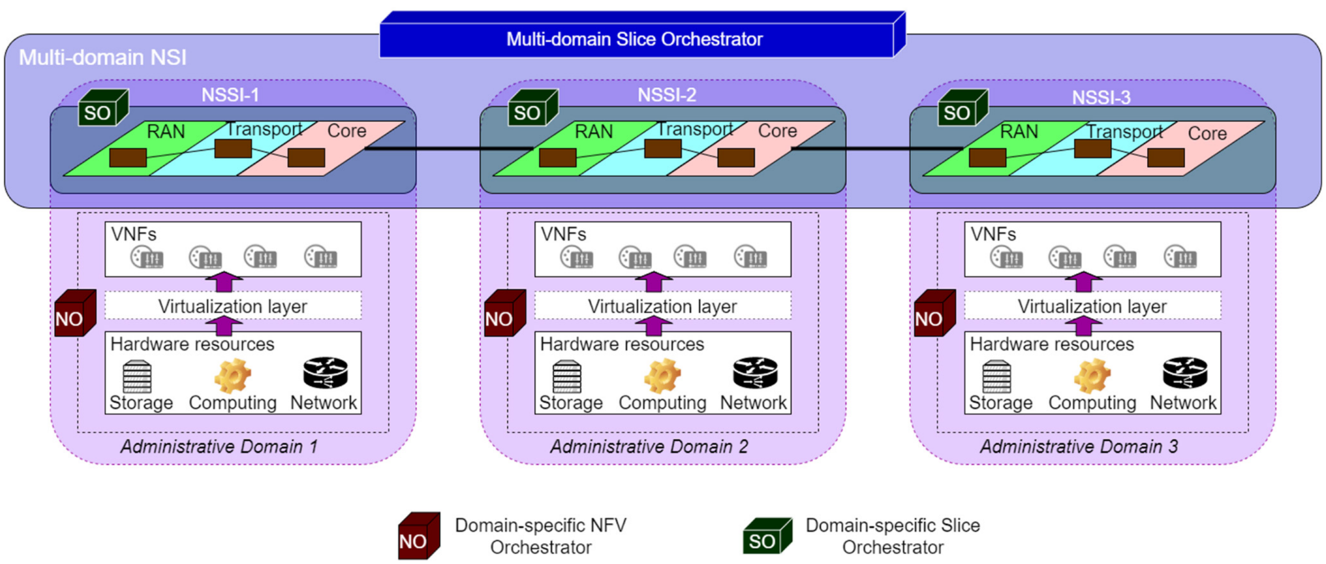

Fig. 19. Multi-domain network slicing.

without expert knowledge. The proposed approach was able to optimise various Wi-Fi parameters per slice dynamically.

C. Multi-Domain and Multi-Operator Slicing

Network slices that are allocated to different vertical applications, may be spread over large geographical areas or encompassing areas where coverage can't be provided by a single operator, may need to combine resources from different operators to provide the coverage [75]. Provisioning of high-quality connectivity infrastructure in specific locations such as schools and transport hubs, the context-driven and location-specific needs for wireless connectivity in different facilities, different business requirements for deployment of 5G networks, and the growing interest for local 5G networks to serve restricted set of customers such as in a factory environment, are some facts that burgeon the concept of local 5G operators concept [235]. Therefore, the involvement of multiple administrative domains in creating and operating the

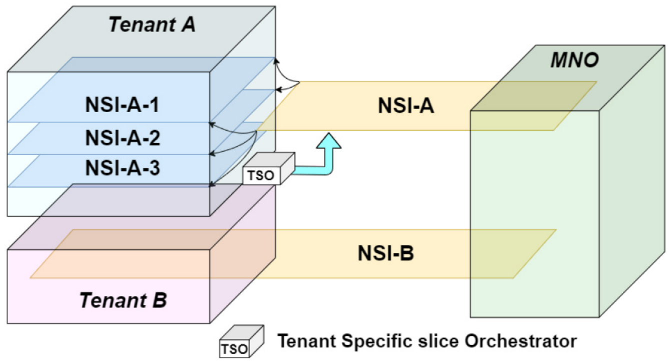

Fig. 20. Hierarchical slicing Architecture.

network slices for providing a better service is a significant requirement in novel 5G networks.

Figure 19 shows the concept of multi-domain network slicing that depicted a network slice spanned over three administrative domains. As shown in the figure, a minimum of three orchestrators are needed to facilitate multi-domain network slicing. One is domain-specific-slice orchestrator for the management and orchestration of the Network Slice Subnet Instances (NSSIs) in each domain. Another is domain-specific-NFVI orchestrator for managing network resources. Thirdly, multi-domain E2E-slice orchestrator for E2E management of the NS. The significant challenges in multi-domain slicing includes identifying the necessary administrative domains with required resources to deploy the NSSIs, stitching them to create the federated NSI, and the run-time coordination of the management operations across different administrative domains [75]. The open-research challenges in the area of multi-domain network slicing are service-management interfaces and service profiling, resource sharing and isolation and service-based network management [75].

D. Hierarchical Slicing

Hierarchical slicing is an exotic area in network slicing that will generate new business models. Ordinarily, MNO creates network slices according to the requirements received from the third party tenants. Though it satisfies the basic communication requirements of the tenant, he may need to further slice the received network slice into more subslices that are specified for separate service areas of the particular tenant. As an example, a giant-sized smart factory can get a dedicated slice from a large MNO. But the factory needs to further slice the received network slice into more slices that are specialised to different applications in the factory, such as operating machines, monitoring the factory environment and communication between employees. This can be recognised as the concept of hierarchical slicing. Reference [236] highlights a set of key features in hierarchical network slicing concepts, such as multi-tenant Virtual Service Networks (VSNs) with embedded slices, hierarchical SDN control and NFV integration and distributed slice selection.

Figure 20 shows the concept of hierarchical slicing. Allocated slice is sliced again into three slices that are specified for the services of the tenant. In [80], Sun *et al.* proposed a hierarchical resource allocation architecture for network slicing. In there, they use Global Radio Resource Manager (GRRM) to allocate resources for a slice and Local Radio Resource Manager (LRRM) that is specific for the slice, to further divide the allocated amount of resources for the slice among the UEs. To the best of our knowledge, there are no significant scientific investigations that were conducted in hierarchical slicing and hence, this is a rich area for conducting future researches.

IX. Conclusion

Network slicing is becoming a reality in future telecommunication networks, due to the support of several technologies, such as SDN, NFV and cloud computing. It has been identified as an inevitable technology in the realisation of the IoT solutions that are proliferating in several applications with heterogeneous network requirements. We comprehensively discussed how network slicing can be used in different IoT applications, along with the existing researches and future research directions for each application. Technical aspects that can be improved in the IoT through network slicing were explored. Although network slicing imparts a lot of advantages in the IoT realisation, several technical challenges in network slicing will mature, due to the evolution of the IoT. We identified those challenges during the survey. Since the lack of large-scale implementations of slicing and the specifications related to network slicing that are still prone to changes, network slicing is a rich area that has several possible future research directions. In all essence, network slicing and IoT are two complementary technologies that, if well harnessed, have the potential of enabling the smart world since 5G networks and beyond.

References

[1] P. F. P. Guillemin. (2009). *The Industrial Internet of Things Volume G1: Reference Architecture*. [Online]. Available: http://www.internet-of-things-research.eu/pdf/IoT Cluster Strategic Research Agenda 2009.pdf
[2] M. Hatton, "The global M2M market in 2013," London, U.K., Machina Research, White Paper, Jan. 2013.
[3] Y. Zhou, F. R. Yu, J. Chen, and Y. Kuo, "Cyber-physical-social systems: A state-of-the-art survey, challenges and opportunities," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 389–425, 1st Quart., 2020.
[4] B. Blanco *et al.*, "Technology pillars in the architecture of future 5G mobile networks: NFV, MEC and SDN," *Comput. Stand. Interfaces*, vol. 54, pp. 216–228, Nov. 2017.
[5] V. W. Wong, *Key Technologies for 5G Wireless Systems*. Cambridge, U.K.: Cambridge Univ. Press, 2017.
[6] W. H. Chin, Z. Fan, and R. Haines, "Emerging technologies and research challenges for 5G wireless networks," *IEEE Wireless Commun.*, vol. 21, no. 2, pp. 106–112, Apr. 2014.
[7] M. Liyanage, A. Gurtov, and M. Ylianttila, *Software Defined Mobile Networks (SDMN): Beyond LTE Network Architecture*. Chichester, U.K.: Wiley, 2015.
[8] M. Jarschel, T. Zinner, T. Hoßfeld, P. Tran-Gia, and W. Kellerer, "Interfaces, attributes, and use cases: A compass for SDN," *IEEE Commun. Mag.*, vol. 52, no. 6, pp. 210–217, Jun. 2014.
[9] Y. Li and M. Chen, "Software-defined network function virtualization: A survey," *IEEE Access*, vol. 3, pp. 2542–2553, 2015.
[10] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Realizing multi-access edge computing feasibility: Security perspective," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2019, pp. 1–7.
[11] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, and T. Taleb, "Survey on multi-access edge computing for Internet of Things realization," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 2961–2991, 4th Quart., 2018.

[12] P. C. Chih and I. Lin, *End to End Network Slicing*, Wireless World Res. Forum, Zurich, Switzerland, 2017.
[13] Nokia, Huawei, and Ericsson, "5G network slicing for vertical industries," Global Mobile Suppliers Assoc., London, U.K., Rep., 2017. [Online]. Available: https://www.huawei.com/minisite/5g/img/5g-network-slicing-for-vertical-industries-en.pdf
[14] "Service requirements for the 5G system: Stage I," 3GPP, Sophia Antipolis, France, Rep. 22.261, Aug. 2016.
[15] "Feasibility study on new services and markets technology enablers network operation," 3GPP, Sophia Antipolis, France, Rep. 22.864, Jan. 2016.
[16] "System architecture for the 5G," 3GPP, Sophia Antipolis, France, Rep. 23.501, Dec. 2016.
[17] "Study on architecture for next generation syste," 3GPP, Sophia Antipolis, France, Rep. 23.799, Dec. 2015.
[18] "Description of network slicing concept," NGMN Alliance, Frankfurt, Germany, Rep., Jan. 2016. [Online]. Available: https://www.ngmn.org/wp-content/uploads/Publications/2016/161010_NGMN_Network_Slicing_framework_v1.0.8.pdf
[19] I. Afolabi, T. Taleb, K. Samdanis, A. Ksentini, and H. Flinck, "Network slicing and softwarization: A survey on principles, enabling technologies, and solutions," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2429–2453, 3rd Quart., 2018.
[20] P. Schulz *et al.*, "Latency critical IoT applications in 5G: Perspective on the design of radio interface and network architecture," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 70–78, Feb. 2017.
[21] A. A. Barakabitze, A. Ahmad, R. Mijumbi, and A. Hines, "5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges," *Comput. Netw.*, vol. 167, Feb. 2020, Art. no. 106984.
[22] A. Kaloxylos, "A survey and an analysis of network slicing in 5G networks," *IEEE Commun. Stand. Mag.*, vol. 2, no. 1, pp. 60–65, Mar. 2018.
[23] Q. Chen and C. Liu, "A survey of network slicing in 5G," in *Proc. Int. Conf. Comput. Sci. Mech. Autom. (CSMA)*, 2017, pp. 27–35.
[24] L. Zhang *et al.*, "A survey on 5G network slicing enabling the smart grid," in *Proc. IEEE 25th Int. Conf. Parallel Distrib. Syst. (ICPADS)*, 2019, pp. 911–916.
[25] 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.
[26] X. Foukas, G. Patounas, A. Elmokashfi, and M. K. Marina, "Network slicing in 5G: Survey and challenges," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 94–100, May 2017.
[27] R. Su *et al.*, "Resource allocation for network slicing in 5G telecommunication networks: A survey of principles and models," *IEEE Netw.*, vol. 33, no. 6, pp. 172–179, Nov./Dec. 2019.
[28] M. Richart, J. Baliosian, J. Serrat, and J.-L. Gorricho, "Resource slicing in virtual wireless networks: A survey," *IEEE Trans. Netw. Service Manag.*, vol. 13, no. 3, pp. 462–476, Sep. 2016.
[29] L. U. Khan, I. Yaqoob, N. H. Tran, Z. Han, and C. S. Hong, "Network slicing: Recent Advances, taxonomy, requirements, and open research challenges," *IEEE Access*, vol. 8, pp. 36009–36028, 2020.
[30] W. Rafique, L. Qi, I. Yaqoob, M. Imran, R. U. Rasool, and W. Dou, "Complementing IoT services through software defined networking and edge computing: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 3, pp. 1761–1804, 3rd Quart., 2020.
[31] X. Zhou, R. Li, T. Chen, and H. Zhang, "Network slicing as a service: Enabling enterprises' own software-defined cellular networks," *IEEE Commun. Mag.*, vol. 54, no. 7, pp. 146–153, Jul. 2016.
[32] V. Sciancalepore, F. Cirillo, and X. Costa-Perez, "Slice as a service (SlaaS) optimal IoT slice resources orchestration," in *Proc. IEEE Global Commun. Conf.*, 2017, pp. 1–7.
[33] Q. Li, G. Wu, A. Papathanassiou, and U. Mukherjee, "An end-to-end network slicing framework for 5G wireless communication systems," 2016. [Online]. Available: arXiv:1608.00572.
[34] V. P. Kafle, Y. Fukushima, P. Martinez-Julia, T. Miyazawa, and H. Harai, "Adaptive virtual network slices for diverse IoT services," *IEEE Commun. Stand. Mag.*, vol. 2, no. 4, pp. 33–41, Dec. 2018.
[35] J. Ni, X. Lin, and X. S. Shen, "Efficient and secure service-oriented authentication supporting network slicing for 5G-enabled IoT," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 3, pp. 644–657, Mar. 2018.
[36] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer*, vol. 50, no. 7, pp. 80–84, Jul. 2017.
[37] S. Antipolis, "Study on architecture for next generation system, release 14," 3GPP, Sophia Antipolis, France, Rep. 23.799, Dec. 2016.
[38] M. A. Habibi, B. Han, and H. D. Schotten, "Network slicing in 5G mobile communication architecture, profit modeling, and challenges," 2017. [Online]. Available: arXiv:1707.00852.
[39] P. Porambage and M. Liyanage, "Security in network slicing," *Wiley 5G Ref: The Essential 5G Reference Online*. Hoboken, NJ, USA: Wiley, 2019, pp. 1–12.
[40] T. Yoo, "Network slicing architecture for 5G network," in *Proc. Int. Conf. Inf. Commun. Technol. Convergence (ICTC)*, 2016, pp. 1010–1014.
[41] S. Staff. (Dec. 2017). *What is Dynamic Network Slicing? What is Dynamic Network Slicing?* [Online]. Available: https://www.sdxcentral.com/5g/definitions/dynamic-network-slicing/
[42] Techopedia. (Jan. 2017). *Scalability*. [Online]. Available: https://www.techopedia.com/definition/9269/scalability
[43] 3GPP. (2016). *Network Sharing; Architecture and Functional Descriptio*. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=830
[44] (Jan. 2020). *The IoT Rundown for 2020: Stats, Risks, and Solutions*. [Online]. Available: https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2
[45] P. Rost *et al.*, "Network slicing to enable scalability and flexibility in 5G mobile networks," *IEEE Commun. Mag.*, vol. 55, no. 5, pp. 72–79, 2017.
[46] Y. Xiao and M. Krunz, "Dynamic network slicing for scalable fog computing systems with energy harvesting," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 12, pp. 2640–2654, Dec. 2018.
[47] M. Jiang, M. Condoluci, and T. Mahmoodi, "Network slicing management & prioritization in 5G mobile systems," in *Proc. Eur. 22nd Wireless Conf.*, 2016, pp. 1–6.
[48] Y. L. Lee, J. Loo, T. C. Chuah, and L.-C. Wang, "Dynamic network slicing for multitenant heterogeneous cloud radio access networks," *IEEE Trans. Wireless Commun.*, vol. 17, no. 4, pp. 2146–2161, Apr. 2018.
[49] A. Mayoral, R. Vilalta, R. Casellas, R. Martinez, and R. Munoz, "Multi-tenant 5G network slicing architecture with dynamic deployment of virtualized tenant management and orchestration (MANO) instances," in *Proc. 42nd Eur. Conf. Opt. Commun.*, 2016, pp. 1–3.
[50] D. Sattar and A. Matrawy, "Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices," in *Proc. IEEE Conf. Commun. Netw. Security (CNS)*, 2019, pp. 82–90.
[51] P. Schneider, C. Mannweiler, and S. Kerboeuf, "Providing strong 5G mobile network slice isolation for highly sensitive third-party services," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.
[52] D. Sattar and A. Matrawy, "Optimal slice allocation in 5G core networks," *IEEE Netw. Lett.*, vol. 1, no. 2, pp. 48–51, Jun. 2019.
[53] A. Mathew, "Network slicing in 5G and the security concerns," in *Proc. 4th Int. Conf. Comput. Methodol. Commun. (ICCMC)*, 2020, pp. 75–78.
[54] T. Haugen, A. A. Hassan, and P. F. Menezes, "Device quarantine in a wireless network," U.S. Patent 9 717 006, Jul. 25, 2017.
[55] V. K. Choyi, A. Abdel-Hamid, Y. Shah, S. Ferdi, and A. Brusilovsky, "Network slice selection, assignment and routing within 5G networks," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2016, pp. 1–7.
[56] P. Porambage, Y. Miche, A. Kalliola, M. Liyanage, and M. Ylianttila, "Secure keying scheme for network slicing in 5G architecture," in *Proc. IEEE Conf. Stand. Commun. Netw. (CSCN)*, 2019, pp. 1–6.
[57] M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, "Internet of Things (IoT): Taxonomy of security attacks," in *Proc. 3rd Int. Conf. Electron. Design (ICED)*, 2016, pp. 321–326.
[58] D. Stiawan, M. Idris, R. F. Malik, S. Nurmaini, N. Alsharif, and R. Budiarto, "Investigating brute force attack patterns in IoT network," *J. Electr. Comput. Eng.*, vol. 2019, Jan. 2019, Art. no. 4568368. [Online]. Available: https://www.hindawi.com/journals/jece/2019/4568368/
[59] N. JOSHI. (May 2019). *8 Types of Security Threats to IoT*. [Online]. Available: https://www.allerin.com/blog/8-types-of-security-threats-to-iot
[60] 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.
[61] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 1, pp. 616–644, 1st Quart., 2020.

[62] S. A. Hamad, Q. Z. Sheng, W. E. Zhang, and S. Nepal, "Realizing an Internet of Secure Things: A survey on issues and enabling technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1372–1391, 2nd Quart., 2020.
[63] *5G Security Recommendations Package# 2: Network Slicing*, NGMN Alliance, Frankfurt, Germany, 2016.
[64] K. Bhardwaj, J. C. Miranda, and A. Gavrilovska, "Towards IoT-DDOS prevention using edge computing," in *Proc. {USENIX} Workshop Hot Topics Edge Comput. (HotEdge)*, 2018. [Online]. Available: https://www.usenix.org/system/files/conference/hotedge18/hotedge18-papers-bhardwaj.pdf
[65] V. A. Cunha *et al.*, "Network slicing security: Challenges and directions," *Internet Technol. Lett.*, vol. 2, no. 5, p. e125, 2019.
[66] *General Data Protection Regulation*. Accessed: Aug. 4, 2020. [Online]. Available: https://gdpr-info.eu/
[67] Y. Zhang, J. Li, D. Zheng, P. Li, and Y. Tian, "Privacy-preserving communication and power injection over vehicle networks and 5G smart grid slice," *J. Netw. Comput. Appl.*, vol. 122, pp. 50–60, Nov. 2018.
[68] F. Z. Yousaf *et al.* "Network slicing with flexible mobility and QoS/QoE support for 5G Networks," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2017, pp. 1195–1201.
[69] (Jul. 2020). *QoS Class Identifier*. [Online]. Available: https://en.wikipedia.org/wiki/QoS_Class_Identifier
[70] D. N. Skoutas, N. Nomikos, D. Vouyioukas, C. Skianis, and A. Antonopoulos, "Hybrid resource sharing for QoS preservation in virtual wireless networks," *Cloud and Fog Computing in 5G Mobile Networks: Emerging Advances and Applications*, vol. 70. Stevenage, U.K.: IET, 2017, p. 303.
[71] M. Höyhtyä *et al.*, "Critical communications over mobile operators' networks: 5G use cases enabled by licensed spectrum sharing, network slicing and QoS control," *IEEE Access*, vol. 6, pp. 73572–73582, 2018.
[72] A. Devlic, A. Hamidian, D. Liang, M. Eriksson, A. Consoli, and J. Lundstedt, "NESMO: Network slicing management and orchestration framework," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2017, pp. 1202–1208.
[73] C. Pereira, A. Pinto, D. Ferreira, and A. Aguiar, "Experimental characterization of mobile IoT application latency," *IEEE Internet Things J.*, vol. 4, no. 4, pp. 1082–1094, Aug. 2017.
[74] S. Redana, A. Kaloxylos, A. Galis, P. Rost, and V. Jungnickel, "View on 5G architecture," Germany, 5G-PPP, White Paper, 2016. [Online]. Available: https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP-View-on-5G-Architecture-For-public-consultation.pdf
[75] T. Taleb, I. Afolabi, K. Samdanis, and F. Z. Yousaf, "On multi-domain network slicing orchestration architecture and federated resource control," *IEEE Netw.*, vol. 33, no. 5, pp. 242–252, Sep./Oct. 2019.
[76] Y. Siriwardhana, P. Porambage, M. Liyanage, and M. Ylinattila, "A survey on mobile augmented reality with 5G mobile edge computing: Architectures, applications and technical aspects," *IEEE Commun. Surveys Tuts.*, early access, Feb. 25, 2021, doi: 10.1109/COMST.2021.3061981.
[77] H. Wang, Y. Wu, G. Min, J. Xu, and P. Tang, "Data-driven dynamic resource scheduling for network slicing: A deep reinforcement learning approach," *Inf. Sci.*, vol. 498, pp. 106–116, Sep. 2019.
[78] M. Leconte, G. S. Paschos, P. Mertikopoulos, and U. C. Kozat, "A resource allocation framework for network slicing," in *Proc. IEEE IEEE Conf. Comput. Commun.*, 2018, pp. 2177–2185.
[79] H. Zhang, N. Liu, X. Chu, K. Long, A.-H. 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.
[80] Y. Sun, M. Peng, S. Mao, and S. Yan, "Hierarchical radio resource allocation for network slicing in fog radio access networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 4, pp. 3866–3881, Apr. 2019.
[81] C. Campolo, A. Molinaro, A. Iera, and F. Menichella, "5G network slicing for vehicle-to-everything services," *IEEE Wireless Commun.*, vol. 24, no. 6, pp. 38–45, Dec. 2017.
[82] C. Campolo, A. Molinaro, A. Iera, R. R. Fontes, and C. E. Rothenberg, "Towards 5G network slicing for the V2X ecosystem," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, 2018, pp. 400–405.
[83] H. Khan, P. Luoto, M. Bennis, and M. Latva-aho, "On the application of network slicing for 5G-V2X," in *Proc. 24th Eur. Wireless Conf.*, 2018, pp. 1–6.
[84] H. Wu, I. A. Tsokalo, D. Kuss, H. Salah, L. Pingel, and F. H. Fitzek, "Demonstration of network slicing for flexible conditional monitoring in industrial IoT networks," in *Proc. 16th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2019, pp. 1–2.
[85] A. E. Kalør, R. Guillaume, J. J. Nielsen, A. Mueller, and P. Popovski, "Network slicing in industry 4.0 applications: Abstraction methods and end-to-end analysis," *IEEE Trans. Ind. Informat.*, vol. 14, no. 12, pp. 5419–5427, Dec. 2018.
[86] V. Theodorou, K. V. Katsaros, A. Roos, E. Sakic, and V. Kulkarni, "Cross-domain network slicing for industrial applications," in *Proc. Eur. Conf. Netw. Commun. (EuCNC)*, 2018, pp. 209–213.
[87] A. Mavrogiorgou, A. Kiourtis, M. Touloupou, E. Kapassa, and D. Kyriazis, "Internet of Medical Things (IoMT): Acquiring and transforming data into HL7 FHIR through 5G network slicing," *Emerg. Sci. J.*, vol. 3, no. 2, pp. 64–77, 2019.
[88] A. H. Celdrán, M. G. Pérez, F. J. G. Clemente, F. Ippoliti, and G. M. Pérez, "Dynamic network slicing management of multimedia scenarios for future remote healthcare," *Multimedia Tools Appl.*, vol. 78, no. 17, pp. 24707–24737, 2019.
[89] E. Kapassa *et al.*, "An innovative eHealth system powered by 5G network slicing," in *Proc. 6th Int. Conf. Internet Things Syst. Manag. Security (IOTSMS)*, 2019, pp. 7–12.
[90] F. K. Santoso and N. C. Vun, "Securing IoT for smart home system," in *Proc. Int. Symp. Consum. Electron. (ISCE)*, 2015, pp. 1–2.
[91] E. Theodoridis, G. Mylonas, and I. Chatzigiannakis, "Developing an IoT smart city framework," in *Proc. IISA*, 2013, pp. 1–6.
[92] B. Dzogovic, B. Santos, J. Noll, V. T. Do, B. Feng, and T. van Do, "Enabling smart home with 5G network slicing," in *Proc. IEEE 4th Int. Conf. Comput. Commun. Syst. (ICCCS)*, 2019, pp. 543–548.
[93] S. Chaabnia and A. Meddeb, "Slicing aware QoS/QoE in software defined smart home network," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp.*, 2018, pp. 1–5.
[94] B. Pokric *et al.*, "Augmented reality enabled IoT services for environmental monitoring utilising serious gaming concept" *J. Wireless Mobile Netw. Ubiquitous Comput. Dependable Appl.*, vol. 6, no. 1, pp. 37–55, 2015.
[95] G. White, C. Cabrera, A. Palade, and S. Clarke, "Augmented reality in IoT," in *Proc. Int. Conf. Service-Oriented Comput.*, 2018, pp. 149–160.
[96] M. F. Alam, S. Katsikas, O. Beltramello, and S. Hadjiefthymiades, "Augmented and virtual reality based monitoring and safety system: A prototype IoT platform," *J. Netw. Comput. Appl.*, vol. 89, pp. 109–119, Jul. 2017.
[97] D. E. Zheng and W. A. Carter, *Leveraging the Internet of Things for a More Efficient and Effective Military*. Lanham, MD, USA: Rowman & Littlefield, 2015.
[98] K. Wrona, "Securing the Internet of Things a military perspective," in *Proc. IEEE 2nd World Forum Internet Things (WF-IoT)*, 2015, pp. 502–507.
[99] L. Yushi, J. Fei, and Y. Hui, "Study on application modes of military Internet of Things (MIOT)," in *Proc. IEEE Int. Conf. Comput. Sci. Autom. Eng. (CSAE)*, vol. 3, 2012, pp. 630–634.
[100] L. A. Grieco *et al.*, "IoT-aided robotics applications: Technological implications, target domains and open issues," *Comput. Commun.*, vol. 54, pp. 32–47, Dec. 2014.
[101] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Commun. Surveys Tuts.*, vol. 14, no. 4, pp. 944–980, 4th Quart., 2012.
[102] M. Yun and B. Yuxin, "Research on the architecture and key technology of Internet of Things (IoT) applied on smart grid," in *Proc. Int. Conf. Adv. Energy Eng.*, 2010, pp. 69–72.
[103] A. I. Sarwat, A. Sundararajan, and I. Parvez, "Trends and future directions of research for smart grid IoT sensor networks," in *Proc. Int. Symp. Sens. Netw. Syst. Security*, 2017, pp. 45–61.
[104] T. Lagkas, V. Argyriou, S. Bibi, and P. Sarigiannidis, "UAV IoT framework views and challenges: Towards protecting drones as "Things"," *Sensors*, vol. 18, no. 11, p. 4015, 2018.
[105] M. Mozaffari, W. Saad, M. Bennis, Y.-H. Nam, and M. Debbah, "A tutorial on UAVs for wireless networks: Applications, challenges, and open problems," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 3, pp. 2334–2360, 3rd Qurt., 2019.
[106] C. Luo, J. Nightingale, E. Asemota, and C. Grecos, "A UAV-cloud system for disaster sensing applications," in *Proc. IEEE 81st Veh. Technol. Conf. (VTC Spring)*, 2015, pp. 1–5.
[107] A. E. Garcia *et al.*, "Performance evaluation of network slicing for aerial vehicle communications," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2019, pp. 1–6.
[108] A. Kamilaris, F. Gao, F. X. Prenafeta-Boldu, and M. I. Ali, "Agri-IoT: A semantic framework for Internet of Things-enabled smart farming applications," in *Proc. IEEE 3rd World Forum Internet Things (WF-IoT)*, 2016, pp. 442–447.

[109] J. Ruan *et al.*, "A life cycle framework of green IoT-based agriculture and its finance, operation, and management issues," *IEEE Commun. Mag.*, vol. 57, no. 3, pp. 90–96, Mar. 2019.

[110] S. R. Shinde, A. Karode, and D. S. Suralkar, "Review on-IoT based environment monitoring system," *Int. J. Electron. Commun. Eng. Technol.*, vol. 8, no. 2, pp. 103–108, 2017.

[111] O. Zakaria, J. Britt, and H. Forood, "Internet of Things (IoT) automotive device, system, and method," U.S. Patent 9 717 012, Jul. 25, 2017.

[112] T. Soenen, R. Banerjee, W. Tavernier, D. Colle, and M. Pickavet, "Demystifying network slicing: From theory to practice," in *Proc. IFIP/IEEE Symp. Integr. Netw. Service Manag. (IM)*, 2017, pp. 1115–1120.

[113] S. Zhang, W. Quan, J. Li, W. Shi, P. Yang, and X. Shen, "Air-ground integrated vehicular network slicing with content pushing and caching," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 9, pp. 2114–2127, Sep. 2018.

[114] *Industry 4.0: The Fourth Industrial Revolution—Guide to Industrie 4.0*. Accessed: Jul. 14, 2020. [Online]. Available: https://www:i-scoop:eu/industry-4–0/#:∼:text=Industry%204:0%20is%20the%20digital;of%20the%20industrial%20value%20chain

[115] T. Qiu, J. Chi, X. Zhou, Z. Ning, M. Atiquzzaman, and D. O. Wu, "Edge computing in industrial Internet of Things: Architecture, advances and challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 4, pp. 2462–2488, 4th Quart., 2020.

[116] A. Gurtov, M. Liyanage, and D. Korzun, "Secure communication and data processing challenges in the industrial Internet," *Balt. J. Modern Comput.*, vol. 4, no. 4, pp. 1058–1073, 2016.

[117] H. Wu, G. T. Nguyen, A. K. Chorppath, and F. Fitzek, "Network slicing for conditional monitoring in the industrial Internet of Things," *Proc. IEEE Softw.*, Jan. 2018, pp. 1–2. [Online]. Available: https://sdn.ieee.org/newsletter/january-2018/network-slicing-for-conditional-monitoring-in-the-industrial-internet-of-things

[118] M. Baddeley, R. Nejabati, G. Oikonomou, S. Gormus, M. Sooriyabandara, and D. Simeonidou, "Isolating SDN control traffic with layer-2 slicing in 6TiSCH industrial IoT networks," in *Proc. IEEE Conf. Netw. Funct. Virtualization Softw. Defined Netw. (NFV-SDN)*, 2017, pp. 247–251.

[119] Y. A. Qadri, A. Nauman, Y. B. Zikria, A. V. Vasilakos, and S. W. Kim, "The future of healthcare Internet of Things: A survey of emerging technologies," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1121–1167, 2nd Quart., 2020.

[120] L. Catarinucci *et al.*, "An IoT-aware architecture for smart healthcare systems," *IEEE Internet Things J.*, vol. 2, no. 6, pp. 515–526, Dec. 2015.

[121] P. S. Ranaweera, M. Liyanage, and A. D. Jurcut, "Novel MEC based approaches for smart hospitals to combat COVID-19 pandemic," *IEEE Consum. Electron. Mag.*, vol. 10, no. 2, pp. 80–91, Mar. 2021.

[122] Y. Siriwardhana, G. Gür, M. Ylianttila, and M. Liyanage, "The role of 5G for digital healthcare against COVID-19 pandemic: Opportunities and challenges," *ICT Exp.*, to be published.

[123] M. S. Hossain and G. Muhammad, "Cloud-assisted Industrial Internet of Things (IIoT)—Enabled framework for health monitoring," *Comput. Netw.*, vol. 101, pp. 192–202, Jun. 2016.

[124] R. Pries, H.-J. Morper, N. Galambosi, and M. Jarschel, "Network as a service—A demo on 5G network slicing," in *Proc. 28th Int. Teletraffic Congr. (ITC)*, vol. 1, 2016, pp. 209–211.

[125] Y. Chang, X. Dong, and W. Sun, "Influence of characteristics of the Internet of Things on consumer purchase intention," *Social Behav. Pers. Int. J.*, vol. 42, no. 2, pp. 321–330, 2014.

[126] M. Boussard *et al.*, "Future spaces: Reinventing the home network for better security and automation in the IoT era," *Sensors*, vol. 18, no. 9, p. 2986, 2018.

[127] Srikanth. (Jan. 2020). *How IoT is Empowering Virtual Reality*. [Online]. Available: https://www.techiexpert.com/how-iot-is-empowering-virtual-reality/

[128] "Empowering consumer-focused immersive VR and AR experiences with mobile broadband," Huawei, Shenzhen, China, Rep., 2016. [Online]. Available: https://www-file.huawei.com/-/media/corporate/pdf/mbb/huawei_whitepaper_vr_ar_final.pdf?la=sw-ke

[129] "VR and AR pushing connectivity limits," Qualcomm, San Diego, CA, USA, Rep., 2018. [Online]. Available: https://www.qualcomm.com/media/documents/files/vr-and-ar-pushing-connectivity-limits.pdf

[130] G. F. Networks. (Apr. 2019). *Cloud AR/VR Whitepaper*. [Online]. Available: https://www.gsma.com/futurenetworks/wiki/cloud-ar-vr-whitepaper/

[131] J. J. A. Esteves, A. Boubendir, F. Guillemin, and P. Sens, "Optimized network slicing proof-of-concept with interactive gaming use case," in *Proc. 23rd Conf. Innovat. Clouds Internet Netw. Workshops (ICIN)*, 2020, pp. 150–152.

[132] Augmented Reality for Enterprise Alliance. (Oct. 2015). *SK Telecom and Ericsson Demonstrate 5G Network Slices for Augmented Reality*. [Online]. Available: https://thearea.org/ar-news/sk-telecom-and-ericsson-demonstrate-5g-network-slices-for-augmented-reality/

[133] P. Grønsund *et al.*, "5G service and slice implementation for a military use case," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, 2020, pp. 1–6.

[134] J. Liu, X. Li, X. Chen, Y. Zhen, and L. Zeng, "Applications of Internet of Things on smart grid in China," in *Proc. 13th Int. Conf. Adv. Commun. Technol. (ICACT)*, 2011, pp. 13–17.

[135] C. Bekara, "Security issues and challenges for the IoT-based smart grid," in *Proc. FNC/MobiSPC*, 2014, pp. 532–537.

[136] F. Kurtz, C. Bektas, N. Dorsch, and C. Wietfeld, "Network slicing for critical communications in shared 5G infrastructures—An empirical evaluation," in *Proc. 4th IEEE Conf. Netw. Softwarization Workshops (NetSoft)*, 2018, pp. 393–399.

[137] N. Dorsch, F. Kurtz, and C. Wietfeld, "On the economic benefits of software-defined networking and network slicing for smart grid communications," *NETNOMICS Econ. Res. Electron. Netw.*, vol. 19, nos. 1–2, pp. 1–30, 2018.

[138] S. Petkovic, D. Petkovic, and A. Petkovic, "IoT devices vs. drones for data collection in agriculture," in *DAAAM International Scientific Book*, vol. 16. Vienna, Austria: DAAAM Int., 2017, pp. 63–80.

[139] A. Rajakaruna, A. Manzoor, P. Porambage, M. Liyanage, M. Ylianttila, and A. Gurtov, "Enabling end-to-end secure connectivity for low-power IoT devices with UAVs," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshop (WCNCW)*, 2019, pp. 1–6.

[140] N. H. Motlagh, M. Bagaa, and T. Taleb, "UAV-based IoT platform: A crowd surveillance use case," *IEEE Commun. Mag.*, vol. 55, no. 2, pp. 128–134, Feb. 2017.

[141] S. Wray. (May 2018). *Autonomous Drone Services Tested Over Intercontinental 5G*. [Online]. Available: https://5g.co.uk/news/drone-services-over-intercontinental-5g/4374/

[142] M. Contento. (Mar. 2020). *Massive IoT and 5G: What's Next for Large-Scale Cellular IoT*. [Online]. Available: https://www.telit.com/blog/massive-iot-5g-whats-next/

[143] P. Chivenge and S. Sharma, "Precision agriculture in food production: Nutrient management," in *Proc. Int. Workshop ICTS Precision Agr.*, 2019, p. 12.

[144] 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.

[145] N. Mangalvedhe, R. Ratasuk, and A. Ghosh, "NB-IoT deployment study for low power wide area cellular IoT," in *Proc. IEEE 27th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC)*, 2016, pp. 1–6.

[146] P. Popovski, K. F. Trillingsgaard, O. Simeone, and G. Durisi, "5G wireless network slicing for eMBB, URLLC, and mMTC: A communication-theoretic view," *IEEE Access*, vol. 6, pp. 55765–55779, 2018.

[147] *The Business Case for MEC in Retail: A TCO Analysis and Its Implications in the 5G Era*. Accessed: Jul. 21, 2020. [Online]. Available: https://builders.intel.com/docs/networkbuilders/the-business-case-for-mec-in-retail-a-tco-analysis-and-its-implications-in-the-5g-era.pdf

[148] S. G. Dacko, "Enabling smart retail settings via mobile augmented reality shopping apps," in *Technol. Forecasting Social Change*, vol. 124, pp. 243–256, Nov. 2017.

[149] H. Sun, Z. Zhang, R. Q. Hu, and Y. Qian, "Challenges and enabling technologies in 5G wearable communications," 2017. [Online]. Available: arXiv:1708.05410v1.

[150] P. Ranaweera, A. D. Jurcut, and M. Liyanage, "Survey on multi-access edge computing security and privacy," *IEEE Commun. Surveys Tuts.*, early access, Feb. 26, 2021, doi: 10.1109/COMST.2021.3062546.

[151] (2018). *The Top 10 IoT Segments in 2018–Based on 1,600 Real IoT Projects*. [Online]. Available: https://iot-analytics.com/top-10-iot-segments-2018-real-iot-projects/

[152] *How Network Latency Affects the Future of Autonomous Vehicles*. Accessed: Jul. 13, 2020. [Online]. Available: https://www.orcad.com/jp/node/6591

[153] *Autonomous Cars Will Generate More Than 300 TB of Data Per Year*. Accessed: Jul. 18, 2020. [Online]. Available: https://www.tuxera.com/blog/autonomous-cars-300-tb-of-data-per-year/

[154] (May 2017). *Putting Sensors to Work in the Factory Environment: Data to Information to Wisdom*. [Online]. Available: https://itpeernetwork.intel.com/putting-sensors-to-work-in-the-factory-environment/#gs.9lkvhx

[155] (2018). *New Ethernet Applications—Industrial Networking Requirements*. [Online]. Available: http://www.ieee802.org/3/ad_hoc/ngrates/public/18_03/woods_nea_01_0318.pdf

[156] *5G in Healthcare: Boosting Remote Brain Surgeries, Connected Health, or Medical VR*. Accessed: Jul. 25, 2020. [Online]. Available: https://medicalfuturist.com/5g-in-healthcare-boosting-telehealth-vr-connected-health/

[157] Q. Zhang, J. Liu, and G. Zhao, "Towards 5G enabled tactile robotic telesurgery," 2018. [Online]. Available: arXiv:1803.03586.

[158] *What Is the Recommended Bandwidth for Different Types of Health Care Providers?* Accessed: Jul. 26, 2020. [Online]. Available: https://www.healthit.gov/faq/what-recommended-bandwidth-different-types-health-care-providers

[159] *Why a Smart Hospital Needs to Look After the Security of Its Network*. Accessed: Jul. 26, 2020. [Online]. Available: https://internationalsecurityjournal.com/why-a-smart-hospital-needs-to-look-after-the-security-of-its-network/

[160] *How Much Internet Speed Does Your Smart Home Need?* Accessed: Jun. 8, 2020. [Online]. Available: Available: https://www:smarthomeblog:net/bandwidthsmart-home/#:∼:text=Speed%3A%20As%20a%20general%20recommendation;you%20can%20adjust%20from%20there

[161] P. Fedchenkov, A. Zaslavsky, A. Medvedev, T. Anagnostopoulos, I. Sosunova, and O. Sadov, "Supporting data communications in IoT-enabled waste management," in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*. Cham, Switzerland: Springer, 2017, pp. 163–174.

[162] E. Mohyeldin. *Minimum Technical Performance Requirements for IMT-2020 Radio Interface(s)*. Accessed: Jun. 20, 2020. [Online]. Available: https://www:itu:int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Documents/S01–1Requirements%20for%20IMT-2020Rev:pdf

[163] *Bandwidth Requirements for Virtual Reality (VR) and Augmented Reality (AR)*. Accessed: Aug. 8, 2020. [Online]. Available: https://www.mushroomnetworks.com/infographics/bandwidth-requirements-for-virtual-reality-vr-and-augmented-reality-ar-infographic/

[164] H. Mendis, P. E. Heegaard, and K. Kralevska, "5G network slicing as an enabler for smart distribution grid operations," in *Proc. CIRED*, 2019, pp. 1–5.

[165] *5G Network Slicing Enabling the Smart Grid*. Accessed: May 25, 2020. [Online]. Available: http://www-file.huawei.com/-/media/CORPORATE/PDF/News/5g-network-slicing-enabling-the-smart-grid.pdf

[166] *Growing Use of UAVs Strains Bandwidth*. Accessed: May 28, 2020. [Online]. Available: https://spacenews.com/growing-use-uavs-strains-bandwidth/

[167] *Enterprise Application of Autonomous UAVs: QoS & QoE From Modern Telecom Networks*. Accessed: Jun. 1, 2020. [Online]. Available: https://www.itu.int/en/ITU-T/Workshops-and-Seminars/qos/201809/Documents/R_Roy_Presentation.pdf

[168] *What Value Can High-Speed Broadband Create for Farming Communities*. Accessed: Jun. 2, 2020. [Online]. Available: https://www.smartfarmnet.com/farming-with-high-speed-broadband.html

[169] I. Afolabi, J. Prados, M. Bagaa, T. Taleb, and P. Ameigeiras, "Dynamic resource provisioning of a scalable E2E network slicing orchestration system," *IEEE Trans. Mobile Comput.*, vol. 19, no. 11, pp. 2594–2608, Nov. 2019.

[170] S. Kukliński and L. Tomaszewski, "DASMO: A scalable approach to network slices management and orchestration," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp.*, 2018, pp. 1–6.

[171] L. Geng, S. Bryant, K. Makhijani, A. Galis, X. de Foy, and S. Kuklinsk. (2017). *Network Slicing Architectur*. [Online]. Available: https://tools.ietf.org/id/draft-geng-netslices-architecture-01.html#rfc.section.3.3.1

[172] C. E. Curtis Collicutt. (2018). *5G Network Slicing and OpenStac*. [Online]. Available: https://object-storage-ca-ymq-1.vexxhost.net/swift/v1/6e4619c416ff4bd19e1c087f27a43eea/www-assets-prod/presentation-media/5G-Network-Slicing-and-OpenStack-Presentation-Copy-C03.pdf

[173] A. Galis. (Nov. 2018). *Network Slicing—A Holistic Architectural Approach, Orchestration and Management with Applicability in Mobile and Fixed Networks and Cloud*. [Online]. Available: http://cnsm-conf.org/2018/files/CNSM18_SlicingTutorial_AlexGalis_5–10-2018.pdf

[174] M. L. Héno, A. Boubendir, and N. Simoni, "Telco network slicing models enabling recursive multi-tenancy," in *Proc. 10th Int. Conf. Netw. Future (NoF)*, 2019, pp. 40–47.

[175] P. Q. Carlos Pignataro. (Apr. 2017). *Service Function Chaining*. [Online]. Available: https://www.cisco.com/c/dam/m/en_us/network-intelligence/service-provider/digital-transformation/knowledge-network-webinars/pdfs/0426-techad-ckn.pdf

[176] S. Raynovich. (Jan. 2016). *What Is Network Service Chaining? Definition*. [Online]. Available: https://www.sdxcentral.com/networking/virtualization/definitions/what-is-network-service-chaining/

[177] S. Zhang, "An overview of network slicing for 5G," *IEEE Wireless Commun.*, vol. 26, no. 3, pp. 111–117, Jun. 2019.

[178] X. Li, J. Rao, H. Zhang, and A. Callard, "Network slicing with elastic SFC," in *Proc. IEEE 86th Veh. Technol. Conf. (VTC-Fall)*, 2017, pp. 1–5.

[179] R. F. Olimid and G. Nencioni, "5G network slicing: A security overview," *IEEE Access*, vol. 8, pp. 99999–100009, 2020.

[180] Y. Khettab, M. Bagaa, D. L. C. Dutra, T. Taleb, and N. Toumi, "Virtual security as a service for 5G verticals," in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2018, pp. 1–6.

[181] L. Suárez, D. Espes, P. Le Parc, F. Cuppens, P. Bertin, and C.-T. Phan, "Enhancing network slice security via Artificial Intelligence: Challenges and solutions," in *Proc. Conf. C&ESAR*, Rennes, France, Nov. 2018. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01959251

[182] (Jul. 2019). *The Evolution of Security in 5G*. [Online]. Available: https://www.5gamericas.org/wp-content/uploads/2019/08/5G-Security-White-Paper_8.15.pdf

[183] Z. Kotulski *et al.*, "Towards constructive approach to end-to-end slice isolation in 5G networks," *EURASIP J. Inf. Security*, vol. 2018, no. 1, p. 2, 2018.

[184] J. Liu, L. Zhang, R. Sun, X. Du, and M. Guizani, "Mutual heterogeneous signcryption schemes for 5G network slicings," *IEEE Access*, vol. 6, pp. 7854–7863, 2018.

[185] L. Suárez, D. Espes, F. Cuppens, C.-T. Phan, P. Bertin, and P. Le Parc, "Managing secure inter-slice communication in 5G network slice chains," in *Proc. IFIP Annu. Conf. Data Appl. Security Privacy*, 2020, pp. 24–41.

[186] F. Meneses, M. Fernandes, D. Corujo, and R. L. Aguiar, "SliMANO: An expandable framework for the management and orchestration of end-to-end network slices," in *Proc. IEEE 8th Int. Conf. Cloud Netw. (CloudNet)*, 2019, pp. 1–6.

[187] M. T. Abbas, T. A. Khan, A. Mahmood, J. J. D. Rivera, and W.-C. Song, "Introducing network slice management inside M-CORD-based-5G framework," in *Proc. IEEE/IFIP Netw. Oper. Manag. Symp.*, 2018, pp. 1–2.

[188] F. Z. Yousaf, V. Sciancalepore, M. Liebsch, and X. Costa-Perez, "MANOaaS: A multi-tenant NFV MANO for 5G network slices," *IEEE Commun. Mag.*, vol. 57, no. 5, pp. 103–109, May 2019.

[189] R. Wen, G. Feng, J. Zhou, and S. Qin, "Mobility management for network slicing based 5G networks," in *Proc. IEEE 18th Int. Conf. Commun. Technol. (ICCT)*, 2018, pp. 291–296.

[190] M. Richart, J. Baliosian, J. Serrati, J.-L. Gorricho, R. Agüero, and N. Agoulmine, "Resource allocation for network slicing in WiFi access points," in *Proc. 13th Int. Conf. Netw. Service Manag. (CNSM)*, 2017, pp. 1–4.

[191] *SliceNet*. Accessed: Aug. 15, 2020. [Online]. Available: https://slicenet.eu/

[192] *AutoAir*. Accessed: Aug. 15, 2020. [Online]. Available: https://www.airspan.com/autoair/

[193] *5G!Pagoda*. Accessed: Aug. 17, 2020. [Online]. Available: https://5g-pagoda.aalto.fi/

[194] *SEMANTIC*. Accessed: Aug. 16, 2020. [Online]. Available: https://cordis.europa.eu/project/id/861165

[195] *MATILDA*. Accessed: Aug. 20, 2020. [Online]. Available: https://www.matilda-5g.eu/index.php

[196] *5G!Drones*. Accessed: Aug. 19, 2020. [Online]. Available: https://5gdrones.eu/

[197] *MonB5G*. Accessed: Aug. 19, 2020. [Online]. Available: https://www.monb5g.eu/

[198] *5GMOBIX*. Accessed: Aug. 21, 2020. [Online]. Available: https://www.5g-mobix.com/

[199] *PRIMO-5*. Accessed: Aug. 21, 2020. [Online]. Available: https://primo-5g.eu/

[200] *5G-MONARCH*. Accessed: Aug. 22, 2020. [Online]. Available: https://5g-monarch.eu/

[201] *5GCity*. Accessed: Aug. 23, 2020. [Online]. Available: https://www.5gcity.eu/
[202] *INSPIRE-5Gplus*. Accessed: Aug. 23, 2020. [Online]. Available: https://www.inspire-5gplus.eu/
[203] *Hexa-X*. Accessed: Jan. 25, 2021. [Online]. Available: https://hexa-x.eu/
[204] J. Martin and J. Bohuslava, "Augmented reality as an instrument for teaching industrial automation," in *Proc. Cybern. Informat. (K&I)*. 2018, pp. 1–5.
[205] I. Malỳ, D. Sedláček, and P. Leitao, "Augmented reality experiments with industrial robot in industry 4.0 environment," in *Proc. IEEE 14th Int. Conf. Ind. Informat. (INDIN)*, 2016, pp. 176–181.
[206] J. Backman, S. Yrjölä, K. Valtanen, and O. Mämmelä, "Blockchain network slice broker in 5G: Slice leasing in factory of the future use case," in *Proc. Internet Things Bus. Models Users Netw.*, 2017, pp. 1–8.
[207] *Why the IoMT Will Start to Transform Healthcare*. Accessed: Aug. 27, 2020. [Online]. Available: https://www.forbes.com/sites/bernardmarr/2018/01/25/why-the-internet-of-medical-things-iomt-will-start-to-transform-healthcare-in-2018
[208] *Using Network Slicing to Enhance Security in e-Health Use Cases*. Accessed: Aug. 28, 2020. [Online]. Available: https://protego-project.eu/2019/05/using-network-slicing-to-enhance-security-in-e-health-use-cases/
[209] *How 5G Mobile Networks are Opening the Door to Remote Surgery*. Accessed: Aug. 28, 2020. [Online]. Available: https://www.medicaldevice-network.com/features/5g-remote-surgery/
[210] *How 5G and Edge Computing Can Enhance Virtual Reality*. Accessed: Aug. 30, 2020. [Online]. Available: https://www.ericsson.com/en/blog/2020/4/how-5g-and-edge-computing-can-enhance-virtual-reality
[211] *5G Network Slicing Enabling the Smart Grid*. Accessed: Aug. 30, 2020. [Online]. Available: http://www-file.huawei.com/-/media/CORPORATE/PDF/News/5g-network-slicing-enabling-the-smart-grid.pdf
[212] S. Sekander, H. Tabassum, and E. Hossain, "Multi-tier drone architecture for 5G/B5G cellular networks: Challenges, trends, and prospects," *IEEE Commun. Mag.*, vol. 56, no. 3, pp. 96–103, Mar. 2018.
[213] *SFC/Network slicing*. Accessed: Sep. 1, 2020. [Online]. Available: https://newslab.iith.ac.in/research/sfc.html
[214] C. Marquez, M. Gramaglia, M. Fiore, A. Banchs, and X. Costa-Pérez, "Resource sharing efficiency in network slicing," *IEEE Trans. Netw. Service Manag.*, vol. 16, no. 3, pp. 909–923, Sep. 2019.
[215] B. Khodapanah, A. Awada, I. Viering, J. Francis, M. Simsek, and G. P. Fettweis, "Radio resource management in context of network slicing: What is missing in existing mechanisms?" in *Proc. IEEE Wireless Commun. Netw. Conf. (WCNC)*, 2019, pp. 1–7.
[216] S. Underwood, "Blockchain beyond bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.
[217] M. Swan, *Blockchain: Blueprint for a New Economy*, Sebastopol, CA, USA: O'Reilly Media, Inc., 2015.
[218] T. Hewa, M. Ylianttila, and M. Liyanage, "Survey on blockchain based smart contracts: Applications, opportunities and challenges," *J. Netw. Comput. Appl.*, vol. 117, Mar. 2021, Art. no. 102857.
[219] A. Chaer, K. Salah, C. Lima, P. P. Ray, and T. Sheltami, "Blockchain for 5G: Opportunities and challenges," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, 2019, pp. 1–6.
[220] *How Blockchain Can Impact the Telecommunications Industry and Its Relevance to the C-Suite*. Accessed: Sep. 5, 2020. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/za/Documents/technology-media-telecommunications/za_TMT_Blockchain_TelCo.pdf
[221] A. Braeken, M. Liyanage, S. S. Kanhere, and S. Dixit, "Blockchain and cyberphysical systems," *Computer*, vol. 53, no. 09, pp. 31–35, Sep. 2020.
[222] 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 Consum. Commun. Netw. Conf. (CCNC)*, 2020, pp. 1–6.
[223] B. Nour, A. Ksentini, N. Herbaut, P. A. Frangoudis, and H. Moungla, "A blockchain-based network slice broker for 5G services," *IEEE Netw. Lett.*, vol. 1, no. 3, pp. 99–102, Sep. 2019.
[224] L. Zanzi, A. Albanese, V. Sciancalepore, and X. Costa-Pérez, "NSBchain: A secure blockchain framework for network slicing brokerage," 2020. [Online]. Available: arXiv:2003.07748.
[225] K. Valtanen, J. Backman, and S. Yrjölä, "Creating value through blockchain powered resource configurations: Analysis of 5G network slice brokering case," in *Proc. IEEE Wireless Commun. Netw. Conf. Workshops (WCNCW)*, 2018, pp. 185–190.
[226] B. Ciszewski. (Oct. 2018). *Machine Learning in Telecommunications: The Sector Bound to Lead the AI Revolution*. [Online]. Available: https://www.netguru.com/blog/ai-in-telecommunications
[227] E. Schmit. (Dec. 2019). *The Powerful Combination of Machine Learning and 5G Networks*. [Online]. Available: https://shape.att.com/blog/combination-of-machine-learning-and-5g
[228] L.-V. Le, B.-S. P. Lin, L.-P. Tung, and D. Sinh, "SDN/NFV, machine learning, and big data driven network slicing for 5G," in *Proc. IEEE 5G World Forum (5GWF)*, 2018, pp. 20–25.
[229] L. Xiao, X. Wan, X. Lu, Y. Zhang, and D. Wu, "IoT security techniques based on machine learning: How do IoT devices use AI to enhance security?" *IEEE Signal Process. Mag.*, vol. 35, no. 5, pp. 41–49, Sep. 2018.
[230] F. Hussain, S. A. Hassan, R. Hussain, and E. Hossain, "Machine learning for resource management in cellular and IoT networks: Potentials, current solutions, and open challenges," *IEEE Commun. Surveys Tuts.*, vol. 22, no. 2, pp. 1251–1275, 2nd Quart., 2020.
[231] A. Thantharate, R. Paropkari, V. Walunj, and C. Beard, "DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks," in *Proc. IEEE 10th Annu. Ubiquitous Comput. Electron. Mobile Commun. Conf. (UEMCON)*, 2019, pp. 762–767.
[232] J. Mei, X. Wang, and K. Zheng, "Intelligent network slicing for V2X services toward 5G," *IEEE Netw.*, vol. 33, no. 6, pp. 196–204, Nov./Dec. 2019.
[233] L. Zhao and L. Li, "Reinforcement learning for resource mapping in 5G network slicing," in *Proc. 5th Int. Conf. Comput. Commun. Syst. (ICCCS)*, 2020, pp. 869–873.
[234] S. De Bast, R. Torrea-Duran, A. Chiumento, S. Pollin, and H. Gacanin, "Deep reinforcement learning for dynamic network slicing in IEEE 802.11 networks," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, 2019, pp. 264–269.
[235] P. Ahokangas *et al.*, "Business models for local 5G micro operators," *IEEE Trans. Cogn. Commun. Netw.*, vol. 5, no. 3, pp. 730–740, Sep. 2019.
[236] (Jul. 2018). *5G and Network Slicing: A New Era in Networking*. [Online]. Available: https://ieee-wf-5g.org/wp-content/uploads/sites/102/2018/11/POLYCHRONOPOLISSlides.pdf

Shalitha Wijethilaka (Student Member, IEEE) received the bachelor's degree (First Class Hons.) in electronics and telecommunication engineering from the University of Moratuwa, Sri Lanka, in 2017. He is currently pursuing the Ph.D. degree with the School of Computer Science, University College Dublin, Ireland. His main research interests include network slicing, network security, and IoT.

Madhusanka Liyanage (Senior Member, IEEE) received the B.Sc. degree (First Class Hons.) in electronics and telecommunication engineering from the University of Moratuwa, Moratuwa, Sri Lanka, in 2009, the M.Eng. degree from the Asian Institute of Technology, Bangkok, Thailand, in 2011, the M.Sc. degree from the University of Nice Sophia Antipolis, Nice, France, in 2011, and the Doctor of Technology degree in communication engineering from the University of Oulu, Oulu, Finland, in 2016. From 2011 to 2012, he worked a Research Scientist with the I3S Laboratory and Inria, Shopia Antipolis, France. He is currently an Assistant Professor/Ad Astra Fellow with the School of Computer Science, University College Dublin, Ireland. He is also acting as an Adjunct Processor with the Center for Wireless Communications, University of Oulu. From 2015 to 2018, he has been a Visiting Research Fellow with the CSIRO, Australia, the Infolabs21, Lancaster University, U.K., Computer Science and Engineering, The University of New South Wales, Australia, School of IT, University of Sydney, Australia, LIP6, Sorbonne University, France, and Computer Science and Engineering, The University of Oxford, U.K. His research interests are 5G/6G, SDN, IoT, Blockchain, MEC, mobile and virtual network security. He was a recipient of prestigious Marie Skłodowska-Curie Actions Individual Fellowship from 2018 to 2020. In 2020, he has received the 2020 IEEE ComSoc Outstanding Young Researcher Award by IEEE ComSoc EMEA. More info: www.madhusanka.com.