KICS The Korean Institute of Communications and Information Sciences

Available online at www.sciencedirect.com

ScienceDirect

ICT Express 7 (2021) 127–137

www.elsevier.com/locate/icte

Driving forces for Multi-Access Edge Computing (MEC) IoT integration in 5G

Madhusanka Liyanage[a,b,*], Pawani Porambage[b], Aaron Yi Ding[c], Anshuman Kalla[b]

[a] School of Computer Science, University College Dublin, Ireland
[b] Center for Wireless Communications, University of Oulu, Finland
[c] Department of Engineering Systems and Services, Delft University of Technology, Netherlands

Received 1 February 2021; received in revised form 15 March 2021; accepted 4 May 2021
Available online 15 May 2021

Abstract

The emergence of Multi-Access Edge Computing (MEC) technology aims to extend cloud computing capabilities to the edge of the wireless access networks, i.e., closer to the end-users. Thus, MEC-enabled 5G wireless systems are envisaged to offer real-time, low-latency, and high-bandwidth access to the radio network resources. Thus, MEC allows network operators to open up their networks to a wide range of innovative services, thereby giving rise to a brand-new ecosystem and a value chain. Furthermore, MEC as an enabling technology will provide new insights into coherent integration of Internet of Things (IoT) in 5G wireless systems. In this context, this paper expounds the four key technologies, including Network Function Virtualization (NFV), Software Defined Networking (SDN), Network Slicing and Information Centric Networking (ICN), that will propel and intensify the integration of MEC IoT in 5G networks. Moreover, our goal is to provide the close alliance between MEC and these four driving technologies in the 5G IoT context and to identify the open challenges, future directions, and concrete integration paths.

Keywords: MEC; IoT; 5G; SDN; NFV; Network slicing; ICN

Contents

* Corresponding author at: School of Computer Science, University College Dublin, Ireland.
E-mail addresses: madhusanka@ucd.ie, madhusanka.liyanage@oulu.fi (M. Liyanage), pawani.porambage@oulu.fi (P. Porambage), aaron.ding@tudelft.nl (A.Y. Ding), anshuman.kalla@ieee.org, anshuman.kalla@oulu.fi (A. Kalla).
Peer review under responsibility of The Korean Institute of Communications and Information Sciences (KICS).

https://doi.org/10.1016/j.icte.2021.05.007

1. Introduction

Internet of Things (IoT) is a thriving ecosystem comprising of massive interconnections of the exponentially increasing number of heterogeneous and resource-constrained physical objects. In its full swing, IoT is geared-up to revolutionize the way we perceive and interact with the world around us. Currently, it supports the myriads of application areas such as healthcare, agriculture, smart cities, automotive, and industries. In the context of IoT applications following is worth to note. On the one hand, the increasing number of IoT applications are designed in such a way that, for data processing and storing, they need to access the centralized cloud computing facility [1]. This is because IoT devices are intrinsically resource-constrained devices (i.e. low battery power, low memory footprints and less processing power). On the other hand, IoT is expected to offer real-time scalable applications with minimal latency and high Quality of Experience (QoE) when required. Thus there is an evident mismatch between the implementation and the expectation.

5G, as an underlying technology, has an indispensable role to play for advancements of numerous other technologies and services, IoT being one of them. In general, 5G use cases are categorized under three broad domains; (i) enhanced mobile broadband, (ii) massive IoT, and (iii) mission-critical IoT. Each category requires different types of network features in terms of mobility, security, policy control, latency, bandwidth and reliability as highlighted in Fig. 1.

The proliferation of new IoT devices to the consumer market will add a higher burden to the mobile network while they access cloud servers. Moreover, the need to access the centralized cloud services via mobile network may limit IoT use cases that demand low latency and high capacity. This brings in the importance of edge computing paradigms in the caliber of MEC, a novel and evolving networking paradigm that is currently standardized by the European Telecommunications Standards Institute (ETSI) [2]. The rationale behind MEC is to extend the capabilities of the cloud to the edge of cellular networks. In principle, this is realized by placing storage and computational resources at the Radio Access Network (RAN) edge, and moving, as and when required, some of the functionalities offered by the cloud to these additional resources at the edge. Some of the typical characteristics of MEC technology are *closest proximity*, *ultra-low latency*, *location awareness,* and *network context information*.

Based on the above discussion, it must be evident that the realization of MEC IoT integration has a huge potential and should be upheld by many underlying technologies. In this article, we examine four key enabling technologies, i.e. Network Function Virtualization (NFV), Software Defined Networking (SDN), Information Centric Networking (ICN) and Network Slicing (NS) and illustrate how to utilize them to accelerate the growth of MEC based IoT systems in 5G networks. Although several other wireless technologies and radio access network technologies are relevant to MEC, we have considered the above key technologies related to the backhaul and core networks of the 5G in this paper.

This paper is structured as follows. Section 2 highlights the key issues and benefits for integrating MEC with IoT. The role of four key enabling technologies NFV, SDN, ICN, NS is discussed in Sections 3, 4, 5, and 6, respectively. Section 7 further illustrates the challenges, integration path, and future directions. Section 8 concludes the present work.

2. MEC-IoT Integration

This section discusses the issues pertaining to IoT and illustrates how MEC based IoT can address them. In particular, the key benefits of MEC, in the context of IoT, are highlighted. Also, the challenges envisioned for MEC-IoT integration are presented.

Undoubtedly, the rapid advancements in IoT are helping the technology to evolve as a mature technology. Nevertheless, factors like simultaneous growth in the number of IoT devices, proliferation in the varied types of IoT applications, and demand to use versatile connectivity options, have given rise to the several issues such as scalability, mobility, latency, power consumption, availability, security and privacy. In general, IoT leverages cloud computing facility which may face several challenges such as the single-point-of-failure, reachability, high wide area network (WAN) latency, and lack of location awareness. In this situation, MEC is geared-up to play an alleviating role by providing many mutual advantages [1,7]. From IoT's viewpoint, MEC furnishes computational resources located very close to IoT devices, thus offering numerous benefits including computation offloading. From MEC perspective, IoT (being the widespread use case of MEC) extends MEC services to all sorts of devices, thereby, it enables wide adoption and evolution of MEC. Furthermore, the cloud infrastructure also gets offloaded. Table 1 summarizes the add-on features that MEC brings-in to overcome many of these issues of different IoT domains.

MEC offers three key benefits for IoT in 5G era. Fig. 1 illustrates the integration of these technologies in 5G networks. The first key benefit that MEC provides is traffic filtering. This is because the requests generated by a multitude of IoT applications are satisfied upfront at the edge of the network, thereby impeding the traffic that otherwise would be pushed upstream towards the cloud facility. Of course, this is the case when the IoT devices do not require services at the global level (e.g., cloud computing capabilities), so they can be served by

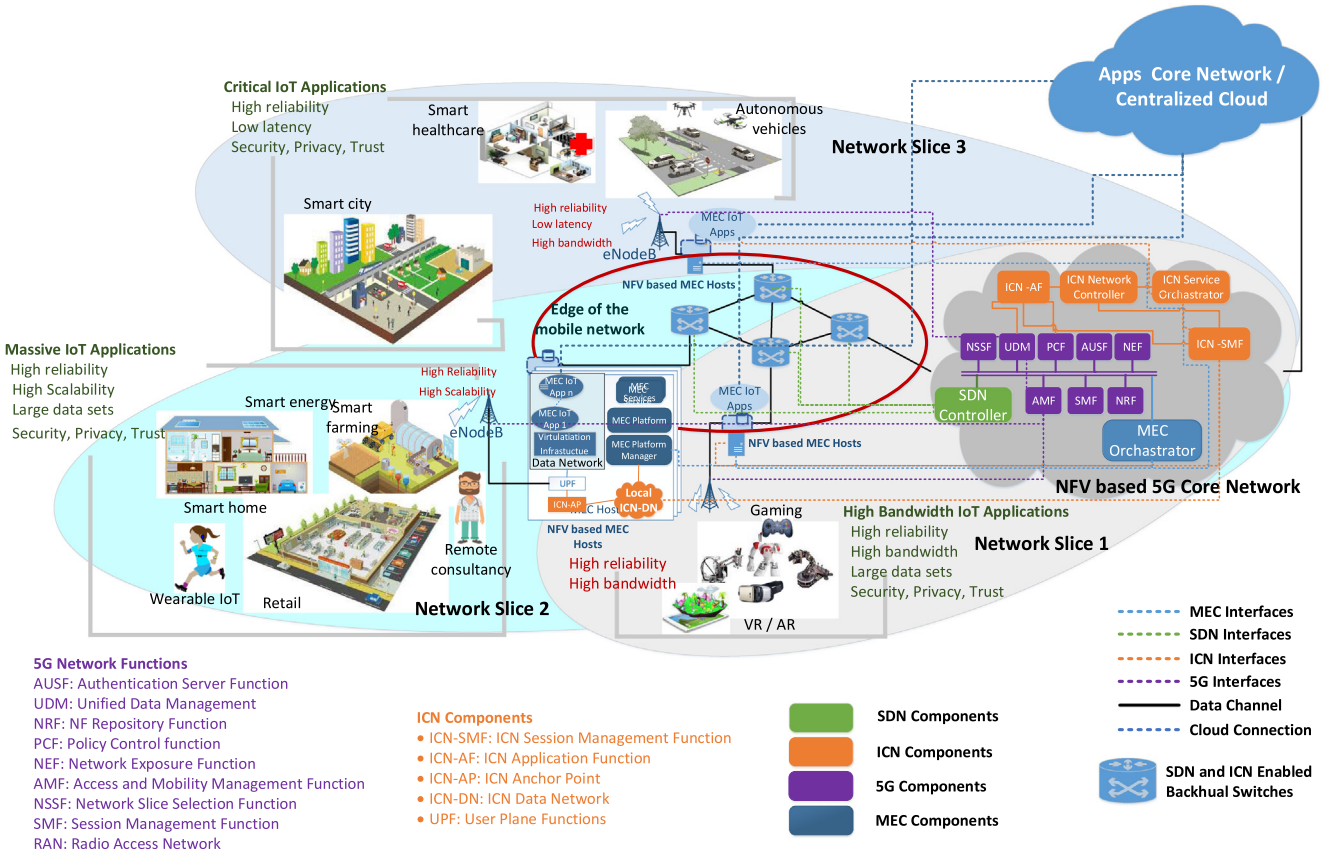

Fig. 1. MEC IoT integration under the umbrella of NFV based 5G core network with SDN, ICN and NS [2–6].

the immediate MEC servers. Thus, using MEC will save cost, reduce the latency and truncate the traffic volume in the core network. The second key benefit is that MEC facilitates accelerated decision making based on the locally processed data, which reduces End-to-End (E2E) delay. This is very important in the critical IoT applications (e.g., remote surgeries, smart grid, autonomous vehicles, and video conferencing), which have very high demands of reliability, availability, and low latency. The third key benefit offered by MEC is enhanced scalability and lifespan of IoT devices. The rapid increase in numbers of IoT connections would proportionally increase the traffic load on the network and decrease the battery life, but thanks to MEC, the battery drain may not increase since less transmission time is required between the IoT device and the MEC server. Besides these three key benefits, MEC offers few other benefits such as context awareness, local storage and caching, support for intermittent connectivity, mobility (fast RAT hand-off), localized privacy and security as presented in Table 1.

Next, we discuss the key challenges that need to be dealt with for MEC-IoT integration. Security, privacy, and trust management are three important synergistic research areas of IoT. Users will be increasingly vulnerable to security threats as more IoT devices and applications make use of the edge facility. The fact that users' data in MEC and IoT are highly exposed, this may lead to many possible ways of a security breach in sensitive data. Typically, the IoT devices are designed with implicit mutual trust, and thus, data sharing happens without a validation process. In such a scenario, where all the devices inherently trust each other and share data, it is difficult to identify a misbehaving device. The situation is aggravated several folds, specially in the absence of a perimeter security mechanism (e.g., firewall) around the network edge. Usually, such security mechanisms can block threats in MEC but are not used in MEC-NVF integration. Thus in MEC systems, it is challenging to identify, authenticate, and authorize devices and the data they generate from the edge to the cloud and back while maintaining a latency of milliseconds' order . Similarly, it is challenging to achieve a non-negligible impact on caching and computation offloading decisions with the user mobility, which will cause frequent handovers among edge servers.

The next few sections elaborate on the cardinal role of four key enabling technologies to achieve the above-mentioned benefits of MEC-IoT integration.

3. Network Function Virtualization

NFV technology utilizes the power of virtualization technologies to decouple physical network equipment from the functions that run on them [8]. Thus, NFV empowers to implement different Virtual Network Functions (VNFs) as software that run on one or more industry standard physical servers. As a result, VNFs can be relocated and instantiated at different physical network locations, as and when required, without the necessity to purchase and install new hardware.

Table 1
The alleviating role of MEC in different IoT domains.

IoT application	Role of MEC	Added characteristics by MEC									
		Low latency	Increased bandwidth	Context awareness	Low power devices (Local storage)	Ability to operate with intermittent connectivity with core network	Fast mobility	Caching	Edge analytics	Private or local network	Localized security and privacy
Smart home	MEC offers reduced communication latency, easy instantiation and fast relocation. Moreover, MEC can process sensitive data locally by preserving the privacy.		✓	✓	✓	✓	✓	✓	✓	✓	✓
Smart city	MEC caters data processing, storing and retrieval requests at the edge of the network thereby provides low latency, high availability, location awareness, mobility management and scalibility.	✓	✓	✓			✓	✓	✓	✓	✓
Healthcare & Remote surgery	EC empowers monitoring and detecting physiological symptoms with uninterrupted communication (even for remote areas) and edge-based analytics. Moreover, the promise of ultra-low latency will furnish technical support to remote-surgeries.	✓	✓	✓			✓	✓	✓	✓	✓
Autonomous vehicles	MEC can improve the operational functions such as real-time traffic monitoring, continuous sensing in vehicles, Infotainment applications and security by fulfilling the latency, reliability, fast big data processing, and throughput requirements.	✓	✓	✓			✓		✓	✓	✓
AR/VR	Migrating computationally expensive tasks to edge servers not only amplifies the computational capabilities of AR/VR devices and elevates the immersive experience of users but also extends their battery-life. Moreover, high capacity and low latency wireless coverage commitments of MEC platforms offer scalability in terms of users who can experience AR/VR even in highly populated areas.	✓	✓	✓			✓	✓	✓	✓	✓
Gaming	MEC can improve user experience for delay-sensitive game users by offloading the resource-intensive applications to the edge servers that are located in the nearest proximity.	✓	✓	✓			✓	✓		✓	
Retail	On-site MEC servers can locally process huge volumes of data generated by different IoT systems such intelligent payment solutions, facial recognition systems, smart vending machines.		✓	✓			✓	✓	✓	✓	✓
Wearables	MEC allows to deploy storage, computing, and caching in close proximity to satisfy wearable requirements such as scalability, short range and low power communication.		✓		✓		✓		✓		✓
Environment monitoring	MEC processes the information closer to sensor and removes the burden of sending raw data over a network with limited bandwidth.			✓	✓	✓		✓	✓		
Farming and poultry	On-site MEC servers can analyze collected big data without real-time uploading to a remote cloud. Thus, MEC can directly reduce the overhead on data access, synchronization and storage.		✓	✓	✓	✓			✓	✓	✓
Smart energy	By performing computations closer to the source of data generation, MEC resolves the issues like traffic congestion, delays due to poor or intermittent connectivity and huge data generation. MEC increases the security and reduces the attack propagation by enforcing security mechanisms closer to the end devices.		✓	✓		✓	✓		✓	✓	✓
Industrial IoT (IIoT)	MEC enabling future IIoT applications by addressing the shortcomings of M2M communication (e.g. latency, peer-to-peer connectivity, resilience, cost, security). Real-time edge analytics and enhanced edge security properties will help to create new IIoT services.	✓	✓	✓			✓		✓	✓	✓

NFV is regarded as one of the key enablers for the deployment of MEC [9] in 5G-IoT networks.

Next, we discuss, how the NFV and MEC technologies can be used together to meet the escalating networking demands of 5G-IoT based services. In the core architecture, both MEC and NFV share similar characteristics. For instance, as depicted in Fig. 2 both MEC and NFV leverage virtualization; the former utilizes it for running applications at edge servers, whereas, later applies it to implement virtualized network functions. Both technologies feature stackable components and each has a virtualization layer. According to ETSI [2], to maximize the return on investment and enhance computing experience, operators may reuse the NVF's infrastructure and its management for hosting MEC as well. In other words, MEC can use the NFVI (NFV Infrastructure) as the virtualization platform to run mobile edge applications alongside other VNFs. Therefore, MEC applications also appear as VNFs in the NFV environment and parts of mobile edge orchestration can be delegated to the NFVO (NFV Orchestration) [3].

4. Software Defined Networking

SDN [10] is an emerging network paradigm that intends to decouple the control plane functions from that of the data plane of a physical networking resource. Moreover, it opposes using vendor specific black-box hardware and instead recommends the use of commodity switches in the data plane. Transferring network control functionalities to the centralized entities has numerous advantages. However, critical IoT applications demand proximity of the SDN controller to the data plane to fulfill low latency constraint. In this regard, MEC can be a pragmatic solution to satisfy the latency requirement. MEC complements the SDN advancements by transforming the mobile network into softwarized networks and ensuring highly efficient network operations and service delivery [4].

Next, we discuss briefly how SDN can support MEC's deployment. SDN can orchestrate the network, its services and devices by hiding the complexities of the heterogeneous mobile environment for the network service developers. Thus, SDN has a significant potential for mitigating the limitations that multi-tier MEC infrastructure tends to face, such as the high complexity of adopting MEC in existing cellular infrastructure.

The SDN control mechanism can lower the complexity of MEC architecture by offering a novel approach that utilizes the available resources more efficiently. SDN can dynamically route the traffic between tier-MEC servers and cloud servers to provide the highest QoS to mobile users. Moreover, SDN paradigm concentrates the network intelligence at the central software-based controller. This will relieve the relatively more straightforward MEC devices from executing complex networking functions such as flow management, service discovery and orchestration.

5. Information Centric Networking

Information Centric Networking (ICN) is a promising clean slate future networking architecture that aims to intrinsically reconcile all the existing issues of TCP/IP networking. ICN advocates a content-centric model in place of the current host-centric model. In contrast with end-to-end principle, ICN takes caching and processing to the core of networks leading to decoupling of contents from their specific locations. Further, the named-content proposition of ICN brings content-consciousness in the network allowing the network to know the details like what content is flowing through it, what is cached, and what is requested. Thus, ICN is another networking paradigm that can intrinsically satisfy the ever-increasing traffic demands along with low latency requirements [11].

Several benefits for 5G-IoT applications can be achieved by exploiting the synergy between MEC and ICN. ICN can solve the issues related to the content delivery and application level reconfiguration in MEC. ICN in the backhaul networks can provide content-consciousness, traffic aggregation (with Pending Interest Table), en-route caching, and forwarding strategy. Thus, it can offer high speed content delivery between the MEC and central cloud systems.

In MEC 5G, when a service is provided by a non-optimal service instance, an application level reconfiguration is performed for optimization [5]. However, such application level reconfiguration can be challenging because it requires session re-initialization. This leads to an increase in session migration delay and adversely affects the IoT applications. Using service-centric networking extension of ICN, the application level reconfiguration delay can be reduced by minimizing the network configuration delay and allowing fast resolution of named service instances [5]. The coexistence of ICN and MEC can also improve the performance of caching offered by edge storage. Numerous ICN features like named-content, context aware and location independent data replication, and data-level integrated security, can benefit both realtime and non-realtime 5G-IoT applications [5].

ICN can significantly improve the efficiency of session mobility in MEC based IoT applications with the optimal operational cost and bandwidth utilization for signaling traffic. In contrast to the IP anchor-based mobility approach, ICN could handle session mobility by using application bound identifier and location split principles which significantly reduces control and user plane overheads.

6. Network Slicing

Network Slicing (NS) is another promising key technology that provides agile networking platforms based on demand and service specifications. It allows multiple logical networks to be created on top of a common shared physical and virtual infrastructure [12].

Integrated use of MEC and NS, along with other technologies, in the realm of 5G will ease different IoT domains. For example consider Massive IoT (MIoT) and delay critical IoT application domains. Massive IoT (MIoT) demands a large number of connections for mostly immobile devices which deal with the exchange of delay-insensitive data. To enable MIoT applications, the network is expected to satisfy the requirements such as edge analytics, reduction in

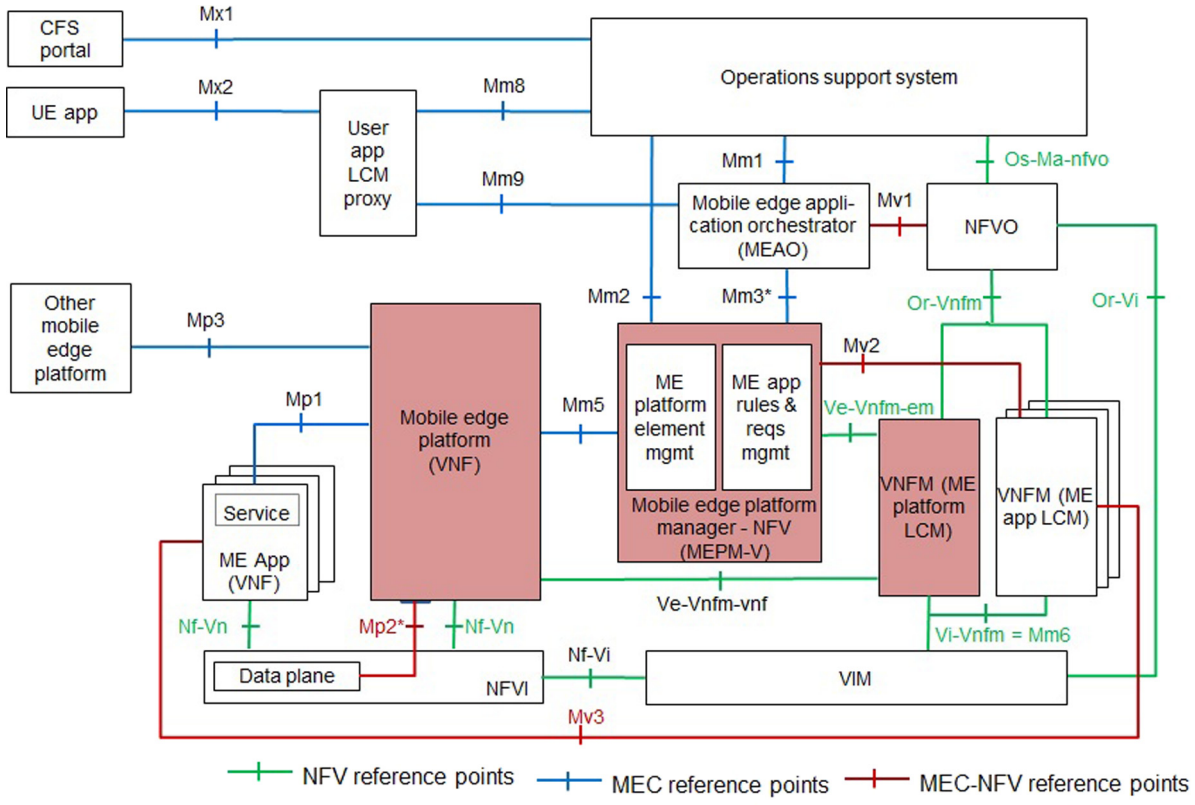

Fig. 2. MEC in NFV Architecture [3].

communication cost, and network scalability. Network slicing coupled with the MEC-based edge analytics and faster security features, can deliver these requirements. MEC provides edge analytics and faster security assets for network slices due to its proximity to the end devices. This will lead to massive cost reduction and the increase in network scalability for the MIoT footprint. On the other hand, delay critical IoT applications, such as autonomous driving, Tactile Internet and industrial Internet, demand ultra low latency, high reliability and traffic prioritization.

In this regard, the powerful combination of MEC and NS can fulfill the demands since latency can be reduced by virtue of MEC and traffic prioritization can be offered by NS. Fig. 3 shows how network slicing can delegate the MEC resources to different slices based on the tenants' demands and achieve efficient network resources utilization. Moreover, NS can enable dynamic and short life cycles for IoT network services.

In 3rd Generation Partnership Project (3GPP) towards full multi-tenancy, MEC has been identified as one of the key technologies to realize the NS extensions. Thus, the synergy between MEC and NS is expected to play a critical role in deploying 5G-IoT applications.

7. Challenges and Future Directions

Table 2 illustrates the pivotal role of the four driving technologies (i.e. SDN, NFV, ICN and NS) to strengthen the IoT requirements enabled by MEC, which in turn helps in realizing the various 5G-IoT applications. In this section, we elaborate on the obstacles, challenges and insights on future research directions pertaining to each of the four driving technologies in the context of MEC-IoT integration in 5G networks.

7.1. NFV

The main research challenges and obstacles for NFV integration are the absence of standards, system complexity in deployment, lack of technical maturity and new security risks. We ponder on each of them in the subsequent discussion.

Currently, NFV is evolving through the phases of implementation and hence demands standardization which should emanate from a collaboration between industry and research communities. In particular, the interfaces and architectural components of NFV should be defined at global level. The absence of this may lead to the rise of compatibility issues which can impede its widespread adaptation.

Most NFV projects encounter a steep learning curve in getting their infrastructure operational up to the expected level. This is due to their heavy dependency on non-standardized implementations. Moreover, due to the lack of technological maturity, updates are released frequently. Thus, maintaining a fully integrated operational deployment model is still hard to accomplish.

Though latency minimization through optimal utilization of resources can be achieved with the efficient deployment of MEC services. However, it is not easy to optimize the MEC services if they depend on complex system components such

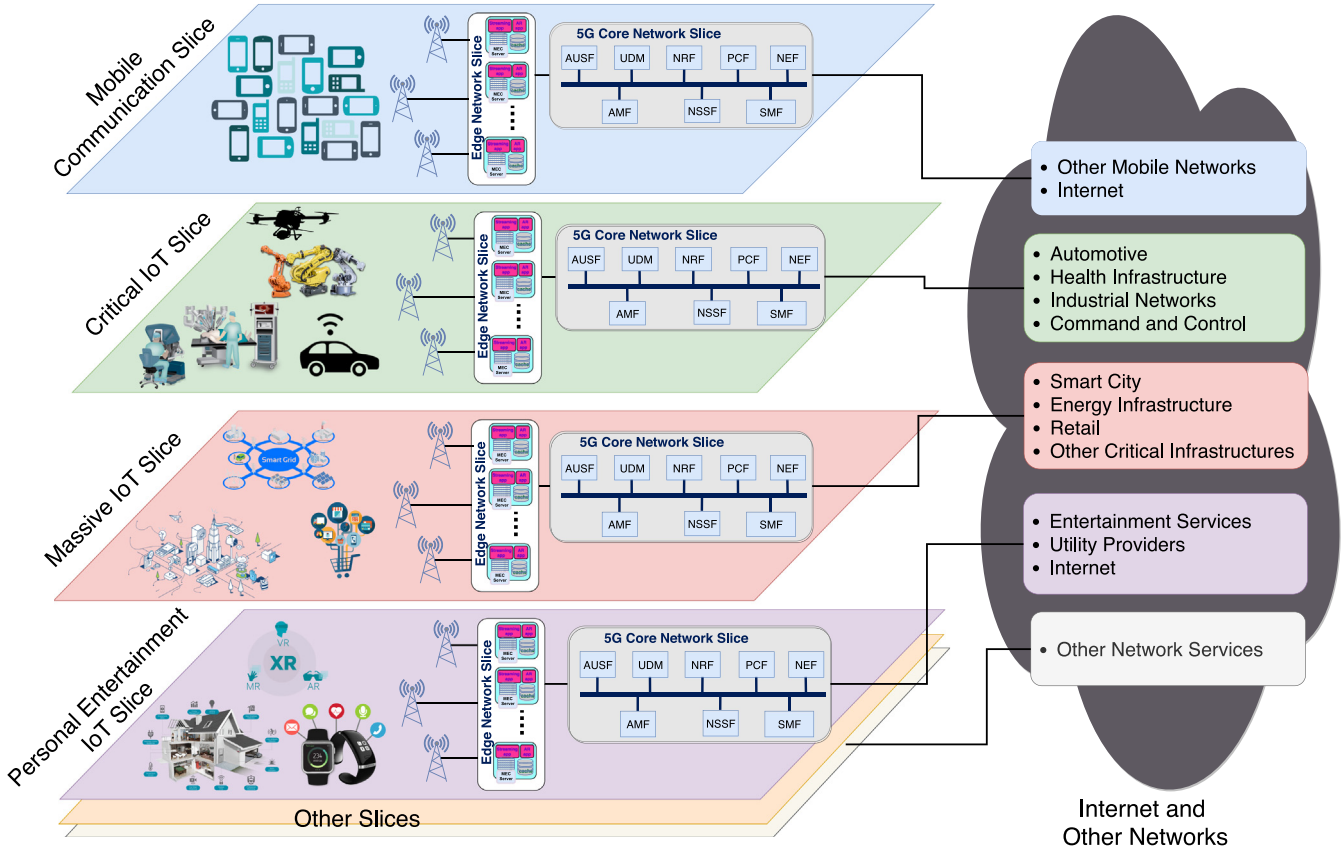

Fig. 3. Use of Network Slicing and MEC in different 5G-IoT applications.

as NFV. The de-facto NFV standard implementations such as OpenStack are difficult to learn, deploy, and use.

NFV integration results in several new security challenges because of the following reasons. On the one hand, MEC introduces software components such as Mobile Edge Platform Manager (MEPM) and Virtual Network Functions Manager (VNFM) to NFV's deployment. These components are not part of the traditional NFV model and create a 'long chain of trust'. On the other hand, NFV features such as resource pooling can lead to sharing security risk between multiple unrelated MEC domains. For instance, an attack on one VNF might hamper other VNFs running on the same Virtual Machine (VM) or physical server.

7.2. SDN

SDN entails several security threats, including SDN protocol weaknesses, information disclosure through interception, flow poisoning, side-channel attacks, and Denial-of-Service (DoS) on SDN controller [10]. In contrast to the traditional black-box type of network devices, SDN uses software programmable common standard backhaul devices. This will not only ease the work of network administrators but also allow malicious attackers to deploy attacks. The integration of SDN with MEC thus becomes challenging since the possibilities of attacks are increasing; on the one hand, the impact of SDN based attacks could result in security degradation of MEC systems and on the other hand, the impact of MEC threats on the open-network based SDN becomes much more devastating.

Furthermore, the inter-working between SDN and MEC will also introduce several connectivity challenges. Similar to SDN southbound, northbound, and east/west interfaces, it would be interesting for MEC also to have three such interfaces, namely, (i) Northbound connections that connect MEC servers to a cloud service (public or private), (ii) Southbound connections, that connect MEC servers and the edge devices and (iii) East/West connections, that connect MEC servers among themselves, so that MEC servers can communicate directly without the need of cloud connectivity. We advocate the necessity to merge similar interfaces to reduce the signaling overhead. Also, the use of too many interfaces makes the security of the network enfeeble. Furthermore, it is indispensable to define clean APIs so that applications and services can program network functions and SDN network to optimize the performance. Such APIs are needed, for instance, to support ultra-low latency applications. Otherwise, information exchange between MEC-IoT and SDN systems will introduce additional delays in network operations.

7.3. ICN

ICN complements MEC since its core functionalities can efficiently govern the interaction between end-users and MEC, especially, in the mobile environment [13]. To achieve the best outcomes of their synergies, proper APIs need to be defined

Table 2
The role of driving technologies to enhance MEC enabled IoT requirements that support 5G-IoT applications.

IoT Requirements enabled by MEC	NFV	SDN	ICN	NS	Related 5G-IoT applications												
					Smart home	Smart city	Remote surgery	Remote health consultancy	Autonomous vehicles	Augmented Reality (AR)	Virtual Reality (VR)	Gaming	Retail	Wearable IoT	Farming	Smart energy	Industrial internet
Support for low latency		✓	✓				✓		✓	✓		✓					✓
Resource optimization	✓	✓		✓		✓	✓		✓	✓	✓	✓	✓	✓		✓	✓
Dynamic resource allocation	✓			✓		✓		✓	✓	✓	✓	✓	✓	✓		✓	✓
Support for edge caching			✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Increased security	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Increased privacy				✓		✓	✓	✓	✓			✓	✓	✓			
Increased scalability	✓	✓	✓		✓			✓					✓	✓	✓	✓	✓
Reduced operational cost	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Increase flexibility	✓	✓		✓	✓	✓			✓	✓	✓	✓	✓	✓	✓	✓	✓
Increase orchestration	✓	✓			✓	✓	✓					✓	✓	✓	✓	✓	✓
Dynamic routing and traffic optimization		✓	✓			✓	✓	✓	✓	✓	✓	✓				✓	✓
Support for fast mobility			✓	✓		✓			✓					✓			✓
Service diversity	✓		✓		✓	✓			✓	✓	✓	✓		✓		✓	✓

in order to communicate between the systems. Though there is on-going research to define NFV and SDN interfaces, however, the interface for ICN communication with MEC-IoT is yet to be defined. This requires collaboration between cross-domain industries as well as standard development organizations.

Furthermore, it is crucial to develop system-level control orchestrator and coordination architecture to enable cooperation between two systems. Moreover, such architecture should focus on autonomic system control rather than the traditional provisioning/configuration or distributed networking systems control.

The real advantages of MEC-IoT can be achieved by obtaining context information such as users' location, other users in the vicinity, condition and resources in the environment. Although ICN can provide different context information (application, network and device level), their simultaneous retrievals are still challenging. Most of the current ICN research is focused on providing the basic functionality rather than utilizing the available context information to improve network parameters such as Quality-of-Service (QoS). For integration, it is required to examine typical scenarios encompassing different IoT and 5G applications (e.g., Tactile Internet, AR/VR, autonomous driving) with varying context.

Another substantial challenge with the use of ICN for MEC supported IoT applications is the difficulty of accomplishing authorization and access control [14]. This is because in ICN, request for named content can be served from any cache-enabled-node as long as the security of the cached content is intact. Thus ICN based communications are unable to make use of traditional user-to-server authentication mechanisms based on Access Control List (ACL). Maintaining an individual access control policy for all the currently available cached contents at each cache-enabled-node across the network tends to incur severe overhands both communication and computation.

7.4. Network slicing

To garner the real benefits of NS in MEC IoT integration, numerous challenges are to be addressed.

The inter-system vertical coordination between NS and MEC IoT integration need to be structured and modeled for efficient information sharing. This vertical coordination can be achieved via two ways. The first method is to define APIs between management systems of slicing and MEC to share the available resources in terms of different IoT applications. The second method is to use physical resource coordination aimed to handle resources through policy and analytics efficiently. However, to synchronize the various research and development activities worldwide, standardization of these interfaces is required.

If NS powered MEC servers can offer fine-grained network functions, it would enhance the scalability to support different vendors. Each coarse grained function at the MEC server can be further divided into many sub-functions. Nevertheless, the challenge is defining the granularity of these networking

Table 3
Technical challenges of MEC-IoT Integration in 5G.

Technical aspect	Issue/Challenge	Description
Communication	Backhaul access	Optimized the communication between MEC servers and remote cloud servers while offloading data/process with higher demand of resources.
	Inter-node communication	Orchestrate the communication among IoT devices, MEC servers, and remote cloud servers when they collaboratively execute multiple jobs.
	Flaws with wireless channels	Multi-path fading, interference, and spectrum shortage should be taken into account for the design of MEC systems to seamlessly integrate computation offloading and radio resource management.
	Limited channel capacity	Wireless and backhaul access links have a limited channel capacity which should be properly shared among mobile devices in a similar way of sharing the computing resources at the MEC server.
Computational offloading	Decision making	MEC servers have to decide whether to execute the relatively simple tasks locally or offload (fully or partially) to the cloud servers. Low power MEC servers may require to offload data more frequently by consuming more backhaul bandwidth.
	Partial offloading	A subset of computations is offloaded to the cloud server considering factors like users or MEC application preferences (e.g., application buffer state), backhaul connections quality (i.e., cloud and MEC servers), MEC server capabilities, cloud capabilities and availability.
	Dependency policies	Define dependency of offloadable components of the applications based on their ability to partition data (e.g., real-time user input has to processed at MEC without offloading) and to predict the execution time/order of multiple tasks. Eg. sequential, parallel, and general dependencies
	Joint computation and communication resource allocation	The main goal comprises the minimization of execution delay to ensure the quality of service at the user end while maintaining high energy efficiency and maximizing the number of served applications. Eg. allocation of single or multiple MEC servers
Mobility management	Connectivity	There is need for smart connectivity with existing networks and context-aware computation using network resources in IoT environments.
	Location management	Under normal circumstances, the location of network nodes is confidential, however in the case of the IoT systems, the location of the nodes needs to be made available without compromising on security.
	Routing group formation	Multiple MEC server clusters have to create different routing groups for different node clusters in the IoT environment.
	Seamless mobility	The seamless execution of applications harnessing capabilities of multiple dynamic and heterogeneous resources to meet quality of service requirements of diverse applications on IoT nodes.
	Mobility context management	Here the idea is to determine the nature of the operations running on the IoT nodes and the latency tolerance level of such operations, hence the mobility management entity is able to determine the optimal mobility handling technique for given use cases.
	Migration	The movement of IoT nodes from one MEC server cluster to another on a more permanent time scale.
Scalability	Deployment independence	The IoT nodes on the MEC server should be capable of conforming to multiple deployment scenarios with little or no modifications to their predefined architectures.
	Resource efficiency	Here the goal is to ensure optimal utilization of networking and computing resources in the MEC system.
	Scalable storing	A huge amount of data will be constantly generated and circulated around the MEC IoT platform, hence there is need for semantic execution environments and architectures that accommodate IoT requirements and scalable storing and communication infrastructure.
	Validity of IoT Scenarios	To this purpose, the validity of the different IoT scenarios should be proven as they may have problems in terms of scalability and adaptability to be applied in such a heterogeneous environment.
Security and trust management	Denial of Service (DoS) attacks	Adversaries attack critical networking or computing resources by sending requests at rates beyond the handling capacity of MEC servers and prevent other nodes from getting access to the resources.
	Man-in-the-Middle (MitM) attacks	In MEC and IoT integration, in the infrastructure layer, the attacker tries to hijack certain segments of the network and begins to launch attacks like eavesdropping and phishing on connected devices. MitM attacks can be launched on multiple VMs.
	VM manipulation	The attacker can be a malicious insider with enough privileges or a VM that has escalated privileges. The adversary begins to launch multiple attacks to the VMs running towards the virtual infrastructures.
	Trust management	Assure the reliability and the trustworthiness among end users, IoT devices and MA–MEC servers.

(*continued on next page*)

functions carefully so that they comply with the available standardized interfaces.

When multiple RATs accommodate the 5G IoT paradigms, there should be some ways to access them on specialized

Table 3 (*continued*).

Technical aspect	Issue/Challenge	Description
Privacy	Harmonize the local privacy policies at global level	When IoTs services are expanding over multiple MEC control regions, it is required to harmonize the privacy at global level.
	Implementation of local and dynamic privacy policies	In current systems, privacy policies and directives are predefined at global level and static over the duration. It is required to find mechanisms to implement local and dynamic privacy policies.
	Foster interoperability	Support technology neutrality by avoiding mandated standards or preferences which could prevent the interoperability.
	Update privacy policies	Existing privacy policies and directives in IoT systems should be modified to support the adaptation of new technologies such as MEC.

or dedicated hardware. Although network slicing may lead to virtualize RAN instances, it is indispensable to ensure radio resource isolation and manage efficiency. To assist RAN virtualization for slicing, Software Defined RAN controllers can be deployed at the MEC servers.

Even though the high-level description of a concrete slice in terms of infrastructure and network functions exists, the physical realization of E2E slice orchestration is yet to be established. MEC servers, as intermediary computing platform between RAN and core network, can play a vital role to support E2E slice orchestration by correlating cloud and radio resources used in different IoT applications.

7.5. Integration path

This section explains integration paths and pinpoints tangible steps to realize the MEC-IoT synergy.

7.5.1. Control level orchestration

To rectify the potential benefits of MEC-IoT enabled 5G networks, different technologies must work simultaneously and in close association as depicted in Fig. 1. However, the fact is, such integration will face difficulty at the control level. Each technology utilizes its orchestrator and management entities such as SDN controller, NFV orchestrator, NS manager and Mobile Edge Platform Manager (MEPM). In this respect, a synergy between these control entities is needed to jointly optimize the network resources and create efficient Service Function Chains (SFCs) for each user application.

7.5.2. Synchronization of standardization process

To achieve orchestration in MEC systems, different technological components need to inter-communicate, which require defining communication interfaces at the architectural-level. However, as of now, the standardization of different technologies is coordinated by different organizations, for e.g., MEC and NFV by ETSI, SDN by ONF, ICN by IETF, IoT by IEEE and Open Internet Consortium (OIC). Therefore, there is an exigency of collaborative synthesized efforts by these standardization bodies. As a good example, ETSI has already started defining the interfaces for NFV and MEC integration (Fig. 2).

7.5.3. Hardware limitations and platform dependencies

The integration of driving technologies demands changes in the control plane, the data plane and hardware/software components. For instance, SDN-enabled switches and devices are needed at the infrastructure layer to implement SDN. Similarly, ICN enabled switches are needed to enable ICN functionalities. Production and installation of such multi-technology hardware will not be easy. To achieve this first, standardization of different technology should be carried out so that vendors can start building such multi-technology hardware equipment. Second, extensive hardware resources are needed to implement multi-technology concepts. Therefore, these hardware limitations and dependencies must be resolved to obtain full benefits of integrating technologies.

7.5.4. AI as a key integration enabler

Recently, Artificial Intelligence (AI) and Machine Learning (ML) have been resorted to create smarter and autonomous wireless systems [15]. In the 5G context, AI can directly benefit the driving technologies such as SDN and NFV to be integrated into MEC and IoT. For instance, AI-based edge orchestrators can be used for better system and host level management functions for various NFV based use cases. AI and MEC together (i.e., edge automation) will combat low latency for real-time IoT services, better orchestration, enhanced security, and backhaul cost savings.

7.6. Additional technical challenges

In addition to the above mentioned challenges, there are several technical challenges of MEC-IoT integration in 5G. These challenges can be categorized under communication, computational offloading, mobility management, scalability, security and privacy. A summary of these technological challenges is presented in Table 3.

8. Conclusion

This paper analyzes the feasibility and practical integration of four technological directions, including NFV, SDN, ICN and Network Slicing, that can facilitate the MEC-IoT integration in 5G mobile networks. Besides highlighting the benefits of using each technology, this paper also identifies the remaining challenges and presents a pragmatic integration paths. We believe these solutions will form a solid ground for

network developers and providers to deploy MEC-IoT in 5G networks optimally.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

This work has been performed under the framework of RESPONSE 5G (Grant No: 789658) project which is funded by European Union and 6Genesis Flagship (grant 318927) project which is funded by the Academy of Finland. The work is also partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 956090, and the iSafe project which is funded by TU Delft Safety & Security Institute.

References

[1] P. Porambage, J. Okwuibe, M. Liyanage, M. Ylianttila, T. Taleb, Survey on multi-access edge computing for internet of things realization, IEEE Commun. Surv. Tutor. (2018).

[2] Y.-C. Hu, M. Patel, D. Sabella, N. Sprecher, V. Young, Mobile edge computing : A key technology towards 5g, ETSI White Paper 11 (11) (2015) 1–16.

[3] Mobile edge computing (MEC); deployment of mobile edge computing in an NFV environment, 2018, [Online]. Available: http://www.etsi.org/deliver/etsi_gr/MEC/001_099/017/01.01.01_60/gr_MEC017v010101p.pdf, ETSI Industry Specification Group (ISG) White Paper.

[4] B. Blanco, J.O. Fajardo, I. Giannoulakis, E. Kafetzakis, S. Peng, J. Pérez-Romero, I. Trajkovska, P.S. Khodashenas, L. Goratti, M. Paolino, et al., Technology pillars in the architecture of future 5g mobile networks: NFV, MEC and SDN, Comput. Stand. Interfaces 54 (2017) 216–228.

[5] R. Ravindran, A. Chakraborti, S.O. Amin, A. Azgin, G. Wang, Realizing ICN in 3GPP's 5G nextgen core architecture, 2017, arXiv preprint arXiv:1711.02232.

[6] N. Alliance, Description of network slicing concept, NGMN 5G P 1 (2016).

[7] F. Bonomi, R. Milito, P. Natarajan, J. Zhu, Fog computing: A platform for internet of things and analytics, in: Big Data and Internet of Things: A Roadmap for Smart Environments, Springer, 2014, pp. 169–186.

[8] R. Mijumbi, J. Serrat, J.-L. Gorricho, N. Bouten, F. De Turck, R. Boutaba, Network function virtualization: State-of-the-art and research challenges, Commun. Surv. Tutor. 18 (1) (2016) 236–262.

[9] L. Gupta, R. Jain, H.A. Chan, Mobile edge computing–an important ingredient of 5g networks, IEEE Software Defined Networks, Newsletter (2016) [Online]. Available: http://sdn.ieee.org/newsletter/march-2016/mobile-edge-computing-an-important-ingredient-of-5g-network.

[10] D. Kreutz, F.M. Ramos, P.E. Verissimo, C.E. Rothenberg, S. Azodolmolky, S. Uhlig, Software-defined networking: A comprehensive survey, Proc. IEEE 103 (1) (2015) 14–76.

[11] A.V. Vasilakos, Z. Li, G. Simon, W. You, Information centric network: Research challenges and opportunities, J. Netw. Comput. Appl. 52 (2015) 1–10.

[12] K. Samdanis, X. Costa-Perez, V. Sciancalepore, From network sharing to multi-tenancy: The 5g network slice broker, Commun. Mag. 54 (7) (2016) 32–39.

[13] D. Grewe, M. Wagner, M. Arumaithurai, I. Psaras, D. Kutscher, Information-centric mobile edge computing for connected vehicle environments: Challenges and research directions, in: Proceedings of the Workshop on Mobile Edge Communications, ACM, 2017, pp. 7–12.

[14] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. Schmidt, M. Waehlisch, Information-Centric Networking (ICN) Research Challenges, IRTF RFC 7927, 2016.

[15] L. Iliadis, I. Maglogiannis, V. Plagianakos, Artificial Intelligence Applications and Innovations, Vol. 520, Springer, 2018.