EURASIP Journal on Information Security

RESEARCH Open Access

Towards constructive approach to end-to-end slice isolation in 5G networks

Zbigniew Kotulski[1], Tomasz Wojciech Nowak[1]*, Mariusz Sepczuk[1], Marcin Tunia[1], Rafal Artych[2], Krzysztof Bocianiak[2], Tomasz Osko[2] and Jean-Philippe Wary[3]

Abstract

Although 5G (fifth generation) networks are still in the realm of ideas, their architecture can be considered as reaching a forming phase. There are several reports and white papers which attempt to precise 5G architectural requirements presenting them from different points of view, including techno-socio-economic impacts and technological constraints. Most of them deal with network slicing aspects as a central point, often strengthening slices with slice isolation. The idea of isolation in the network is not new. However, currently considered technologies give new capabilities that can bring added value in this field. The goal of this paper is to present and examine the isolation capabilities and selected approaches to its realization in network slicing context. As the 5G architecture is still evolving, the specification of isolated slices operation and management brings new requirements that need to be addressed, especially in a context of end-to-end (E2E) security. Thus, an outline of recent trends in slice isolation and a set of challenges are presented. The challenges, if properly addressed, could be a step from the concept of 5G networks to proof-of-concept solutions which provide E2E user's security based on slices isolation. Among other things, the key features are proper slice design and establishment, security at interfaces, suitable access protocols, correct virtual resources sharing, and an adaptable management and orchestration architecture (MANO). In conclusion of the paper, short outlines of two of the main secure isolation challenges are given: a proper definition of isolation parameters and designing suitable MANO system.

Keywords: Slicing, Slice chaining, Slice orchestration, Isolation in sliced network, 5G networks

1 Introduction

Stage of work on the 5G network architecture can be characterized as the moment of transition from storming phase to forming phase. There is a wide range of ongoing projects related to different areas of the 5G network in 5G Infrastructure Public-Private Partnership (5G PPP) [1]. Hence, there are several main approaches to the architecture and implementation. Many 5G PPP phase 1 projects deal with network slicing aspects considering both technology and business perspectives. The CHARISMA (Converged Heterogeneous Advanced 5G Cloud-RAN Architecture for Intelligent and Secure Media Access) [2] project introduces a new approach to routing and a virtualized architecture that focuses on two domains: mitigation of offload with the shortest path, which is close to end users and ensuring an end-to-end security services chain realized by virtualized open access physical layer security (PLS). These novel cross-layer approaches to security address such areas as: data confidentiality, data integrity, provider's resources isolation, and authentication and authorization. The security aspects of 5G networks are discussed in 5G-ENSURE project [3]. Main goals of the initiative focus on developing non-intrusive security and privacy mechanisms, which will ensure the following: AAA services, privacy, trust, network management and monitoring, and virtualization isolation for the core 5G architecture. Within the project, the 5G security testbed with proposed security components was demonstrated. The 5G NORMA (Novel Radio Multi-service adaptive network Architecture) [4] project has the key objective to develop a novel, adaptive, and future-oriented 5G mobile network architecture. The created architecture should provide network customizability and, at the same time, ensure meeting requirements associated with rigorous performance, energy saving, cost

*Correspondence: T.Nowak@tele.pw.edu.pl
[1] Institute of Telecommunications of WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland
Full list of author information is available at the end of the article

reduction, and security. Very similar goal has the 5G-Crosshaul Project [5]. It aims to create a 5G transport network solution which will be integrated with fronthaul and backhaul parts of the network. Finally, the results of the research should give adaptive, programmable, and cost-efficient ideas for advanced services. The 5GEx (5G Exchange) project [6] refers to enabling cross-domain orchestration of services, which allow end-to-end network and service elements to connect in a multi-vendor heterogeneous technology and in different resource environments. The project ensures using NFV/SDN (Network Function virtualization/Software Defined Network) technologies to produce an open platform enabling cross-domain orchestration of services, which can be tested with a sandbox networking idea (tests should include the created architecture, mechanisms, and a business model). The other two projects which are worth mentioning are METIS-II [7] and Flex5Gware (flexible and efficient hardware/software platforms for 5G network elements and devices) [8]. The first project applies to developing the overall 5G Radio Access Network and providing different technical mechanisms needed for integration of many types of 5G technologies and components. The second one concentrates on creating flexible and reconfigurable hardware together with software for network elements and devices, considering problems connected with capacity, energy efficiency, and scalability.

The 5G-PPP is now in its second phase where new projects were launched in June 2017. SliceNet project [9] intends to meet the requirements from the management and control planes of network slicing across multiple administrative domains, facilitating early and smooth adoption of 5G slices for verticals to achieve their demanding use cases, and managing the QoE for slice services. The use of end-to-end network slicing mechanisms to allow sharing the infrastructure among multiple operators/vertical industries and customizing its capabilities on a per-tenant basis is covered by 5G ESSENCE [10]. In this approach, network abstraction and virtualization will serve as key enabling technologies for delivering consistent network isolation allowing 5G actors to operate virtual networks on top of the physical infrastructures, with virtual resource isolation and virtual network performance guaranties, enabling the delivery of the Network-as-a-Service and providing the flexibility needed to provision network resources.

The 5G-MoNArch project [11] is dealing with Inter-slice control and cross-domain management, to enable the coordination across slices and domains, while Matilda [12] develops Intelligent and unified orchestration mechanisms for the automated placement of the 5G-ready applications and the creation and maintenance of the required network slices.

The concept of 5G!Pagoda project [13] has the principal goal of federating Japanese and European 5G testbeds to create essential standards and to clarify views on 5G Mobile Network Infrastructure, which can be used to dynamic deployment and management of network slices for various types of services. Moreover, the project focuses on creating a scalable 5G network slicing architecture [14], including a multi-tenancy aspect of using resources, slice management and orchestration, and separation of control and data planes.

The standardization of 5G is gaining momentum, too. ITU (International Telecommunication Union) during works on next-generation networks created focus group FG IMT-2020 [15] to identify wireless standards shortcomings, which should be improved in the development of International Mobile Telecommunication (IMT) for 2020 and further 5G networks. The group produced several deliverables, which can be used in future researches. By the end of 2017, 3rd Generation Partnership Project (3GPP) Release 15 of the 5G system architecture has been defined with overall 5G system architecture, its features, functionality, and services including network slicing, see [16–18].

Concept of isolation in the network is not new. However, currently considered technologies give new capabilities that can bring new value in this field. For example, isolation considered as security enabler depends on the quality of isolation mechanisms used in the various components of the network. In 5G networks, there will be rather a portfolio of isolation technologies available than single one, like a Virtual Private Network (VPN). This means that it will be necessary to integrate and manage a variety of isolation mechanisms on different levels. Basing on the assumption that isolation techniques are among important enablers for security in 5G, the analysis of isolation capabilities and selected approaches to its realization in network slicing is presented. Isolation abilities refer in our E2E approach to each of the following domains:

- Radio Access Network (RAN), considering air interfaces;
- Core Network (CN), including virtualization technologies;
- Gi-access to different service providers.

On the one hand, it is important to identify native isolation capabilities, but on the other hand, it is also necessary to propose improvement of existing concepts and to identify the missing parts.

Considering agile but secure solutions, one can notice existence of opposite poles. At one end, there are demanding business requirements, especially in relation to 5G network; at the other end, there are technical conditions that must meet the expectations without breaching security standards. Business perspective has determined expected network parameters and introduced more open approach to network management. It forced changes that have positive impact from the client perspective. Multi-vendor and multi-tenant network concept based on automation and elasticity is real way to meet the needs but brings new challenges at the same time, introducing new potential vectors of attack. One of the most difficult challenges concerns isolation in relation to Quality of Service (QoS) and Quality of Experience (QoE). At the same time, expected QoS/QoE should be preserved with proper Quality of Security. If it fails, users of the network can request a return to the rigid mechanisms which can cause the collapse of the concept of programmable, open networks as such. Therefore, realization of elasticity and agility is strongly connected with isolation technologies supporting security. Isolation level should be considered as an important parameter determining service realization in future networks.

The goal of this paper is to examine the isolation capabilities and selected approaches for its realization in network slicing context. As the 5G architecture is still evolving, specification of isolated slices operation and management bring new requirements that need to be addressed.

The rest of the paper is structured as follows: Section 2 provides brief overview of challenges for 5G networks; in Section 3, there are presented known network slicing concepts; Section 4 presents further details about isolation techniques and network slicing management; Section 5 summarizes known research problems related to 5G software-defined ecosystem and slicing; Section 6 presents new perspective of designing sliced environment and providing E2E slices isolation in 5G networks; Section 7 presents types of isolation and isolation parameters; Section 8 gives a draft presentation of the ETSI MANO (European Telecommunications Standards Institute Management and Orchestration Architecture) possible extensions to face 5G challenges; and finally, in Section 9 conclusions and future research perspectives are presented.

2 Slicing: the 5G challenge

The new (5G) network concept will be more focused on business aspects than previous generations of mobile networks. Sets of requirements described in [19–22] are very difficult or expensive to be satisfied in the whole network at the same time (e.g., the bandwidth over 300 Mbps, very small latency of few milliseconds and support up to 200,000 devices/km^2 with 99.999% reliability level). However, it is feasible to provide some subsets of such requirements, and a network operator can configure multiple logical networks with different network efficiencies and properties. This is the reason for splitting one physical network into multiple logical networks. Such a 5G-based virtual environment will provide a platform for services with specific properties (Key Performance Indicators, QoS/QoE parameters, etc.), which can be used to define new logical networks [23]. Each of these networks has its own dedicated application (voice communication, video streaming, Internet of Things, e-health, etc.) and its own properties based on business requirements for each service, which will be provided over this network [19, 24, 25]. In the whole set of requirements with high probability exist many subsets of properties, which cannot be satisfied at the same time. There exist several different reasons for that, e.g., expensiveness, limitations of current technologies, physical limitations, etc. However, now a network operator usually has the general-purpose network, which should satisfy all requirements, which is more difficult than satisfying only some of them. Reducing the set of requirements for a logical network could improve selected properties that are critical for the service provided over this network.

2.1 The isolated slices

The logical networks described above are the core of the network slicing concept. In this concept, the network and available resources can be partitioned in many slices, which are associated with services and sets of requirements. Each slice can be considered as (at least) one logical network. Network slicing is usually considered together with orchestration concept, which supports slice management (creating slices, changing slices' properties, reconfiguration of slice's network, etc.) and provides interfaces (northbound interface, API—application programming interface) for service providers, other network operators, and other allowed (authorized) users. The purpose for this feature is to make services and networks more agile and adjustable to business and user's requirements or current network situation.

In this paper, the slice isolation concept is considered as a special form of generic slicing idea, which could be attractive for network operators and users. More exact meaning of the isolation property is explained in Section 4.

2.2 Security in sliced network

This new concept by introducing new elements brings new security challenges as these new elements could cause new security threats. It is important to define who and how can use orchestrator (and other modules, which allow changes in network via interface) to avoid security threats like exhaustion of resources or Denial of Service (DoS) attack. The slicing concept itself is a source of security issues. Systems which support slicing may be exploited by attackers. Slicing could also use heterogeneous platforms (because it can be implemented in different layers and on different levels of abstraction) and solutions: slicing components can be implemented in firmware, on OS kernel level (e.g., as a kernel module), in the virtualization software systems (e.g., as a part of virtualization environment or a plug-in for virtualization system, which supports communication between a slice and selected host's applications, like orchestrator or other part of the management layer) or even in the regular software. In this wide spectrum of environments, the slicing components may be provided by different vendors. Ensuring a common level of security for all applications, which build slicing concept in this case, can also be difficult.

Adding special properties to slices (isolation, protection, etc.) might create new attack methods by exploiting weakness of an isolation providing system to reach resources assigned to another slice with better parameters in order to lower costs or to intercept sensitive data stream. An attack on these properties could also be a part of a more complex attack scenario (it could be the subject of an attack in the Attack Jungle concept [26]).

In slicing for 5G, there are some common network services or functions like mobility management or AAA (Authentication, Authorization, Accounting) service [27], which are shared among several slice instances. This concept is in contrary with the isolation property and one should consider how to solve this problem, especially in 5G, where there are more shared functions than in traditional wired networks.

2.3 The major challenge in sliced 5G network

The key problem in 5G networks is implementation of the 5G RAN. The solution for some related problems could be using small cells in the mmWave [28]. Attenuation in this frequency band is bigger than in regular wireless networks (2G- 4G), but in some windows, the propagation parameters are good enough to provide small cell with 200 m range [28]. This property naturally isolates traffic between different cells. Using two types of cells enables the architecture, where part of data is transmitted by macro cells (e.g., data from C-Plane—Control Plane, what has been described in [28]) and the rest of them is transmitted by small cells (e.g., data from U-Plane—User Plane). In the slicing terms, one can look at this as a special meta-slice, which allows user equipment (UE) to communicate with RAN and CN.

However, not all new solutions have this positive effect on isolation level or naturally enable slicing in a network. For instance, NOMA (non-orthogonal multiple access) assumes that more than one UE receives a message on the same frequency channel, code, and time slot [28], and it recognizes messages depending on the signal power level. In this case, the e-NodeB must consider UEs membership in slices while frequencies, codes, and time slots are assigned to avoid the isolation violation. Another technology, which could be useful in 5G networks, but which provides new isolation problems, is cognitive radio [28]. It allows in some cases to use non-dedicated frequency band for communication. This band is shared with other systems (not only mobile networks but also military networks, radio, TV systems, etc.) and a 5G's UE (or a RAN node) is only a secondary user, which can use this band only when it is unused. The primary user can preempt the secondary user, which means that one must consider not only isolation between slices, but also isolation between a slice and other systems.

2.4 Minor problems

Network slicing and slicing isolation in the 5G networks causes many open questions related to rights to manage specific elements of the network, slices creation and isolation, services and slices chaining, network sovereignty, etc. In the following sections an attempt is made to answer some of them or at least precise new related challenges.

3 Concepts of network slicing

3.1 Network slicing definition

Network slicing is one of the crucial technologies that enables flexibility and scalability and that improves security as it allows creation of multiple separated logical networks spanned over a shared hardware infrastructure. First idea of network virtualization and slicing has been introduced in the paper [29], where the authors described an overlay network, the PlanetLab, which was able to produce slices of the network to provide environment for simultaneous design and utilization of different services. Since then this concept has grown considerably and has become the subject of extensive investigations. In recent studies and designs, the network slicing idea is based on the three-layers model [30] (see Fig. 1):

- Service instance layer;
- Network slice instance layer;
- Resource layer.

The Service Instance Layer describes the services (e.g., business services or end-user services) which should be supported. Each service is created as a Service Instance. Usually a service can be provided by a network operator or third parties, so the Service Instance can consist of by both operator's services and third parties' services.

A network slice instance is a set of (virtualized) network functions implemented at resources which enable running these network functions. It forms complete instantiated logical networks that meet certain network characteristics (e.g., ultra-low-latency, ultra-reliability, etc.) required by the Service Instance. A network slice instance could be isolated from another network slice instance in several ways, e.g., full or partial isolation and logical or physical

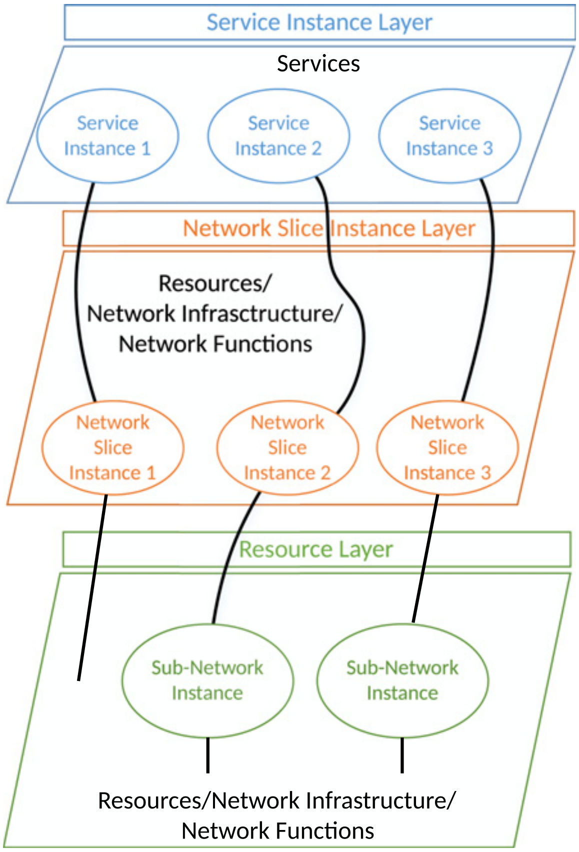

Fig. 1 Network slicing layers, based on [30]

isolation. To create a network slice instance, a network operator uses a Network Slice Blueprint (description of the structure, configuration, and the flows and ways to control the network slice instance during its life cycle). A network slice instance ensures the network characteristics which are needed by a service instance. Therefore, a network slice instance can be shared with multiple service instances provided by the network operator. The network slice instance layer contains many instances of network slices.

The resources layer contains both physical and logical resources. The network slice instance can consist of sub-network instances, which can be shared with multiple network slice instances. The network slice instance is defined by a Network Slice Blueprint. For creating every network slice instance are required dedicated polices and configurations.

3.2 Vertical and horizontal slicing

Another slicing concept is described in [31], where the authors describe two approaches to network slicing: vertical and horizontal. In case of vertical network slicing, one network is sliced into multiple network slices, each designed and optimized for services or applications. The horizontal network slicing enables sharing of resources between nodes and network devices. Both approaches can be implemented simultaneously and they can work together.

3.3 E2E network slicing

The concept of network slicing in 5G refers to three areas [32, 33]:

- Network slicing in the air interface;
- Network slicing in the RAN;
- Network slicing in the CN.

3.3.1 Network slicing in the air interface

The idea of network slicing of air interface (see Fig. 2) refers to proper partitioning of physical radio resources (PHY layer), mapping them into logical resources, and creating the operations of MAC (medium access control) and higher layers based on the logical PHY resources.

3.3.2 Network slicing in the RAN

The network slicing in the RAN describes an optimal configuration of Control Plane and User Plane considering the specificity of slice. Moreover, two aspects should be investigated:

- The Radio Access Type (RAT) which supports services provided by a slice.
- The proper configuration of RAN capabilities with interfaces. It applies also to a correct cell deployment in every slice based on requirements (see Fig. 3). Based on factors such as QoS requirements, traffic load, or type of traffic, the RAN architecture should be properly tailored to each slice. For example, due to RAN configurations every slice uses different kinds of cells: slice 1 uses only macro cells, slice 2 only small cells, and finally, slice 3 uses both macro and small cells. In other scenario, slice 1 can work with macro and small cells, meanwhile slice 3 uses only small cells.

This is a complex challenge as some goals associated with 5G usage cannot be met at the same time (e.g., low latency and high reliability usually have an impact on the spectral efficiency).

Some recent attempts to obtain a system that enables the dynamic on-the-fly virtualization of base stations, the flexible customization of slices to meet their respective service needs and which can be used in an E2E network slicing has been presented in [34]. The system gives the functional and performance isolation of slices, while allowing for the efficient use of RAN resources among them.

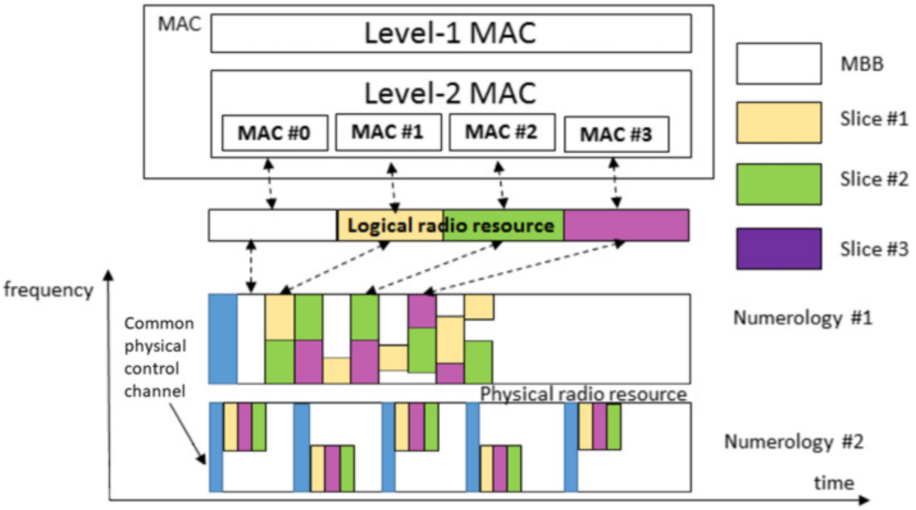

Fig. 2 Network slicing of air interface, based on [31]

3.3.3 *Network slicing in the CN*

Network slicing in CN is possible due to two technologies: Network Function Virtualization (NFV) and Software Defined Networking (SDN). The goal of SDN is to separate the control plane from the data plane. Moreover, the control plane should be programmable through APIs to introduce flexibility of management. Supporting the SDN-like separation of planes is one of the main principles of 5G core network architecture, because it allows [35]:

- Data and control resources to be scaled independently.
- Data plane closer to the users' devices.
- Appropriate choice of the data plane function required for different slices.
- Decomposition of data plane into smaller functions.
- Possibility of migration to cloud deployments.

The goal of NFV is to virtualize network functions into software applications that can be run on standard servers or as virtual machines running on those servers.

4 Network slicing: creation, isolation, management, security

4.1 Architecture and slices creation

The problem of creation of 5G network slicing is the fundamental one, so it is extensively studied in the lit-

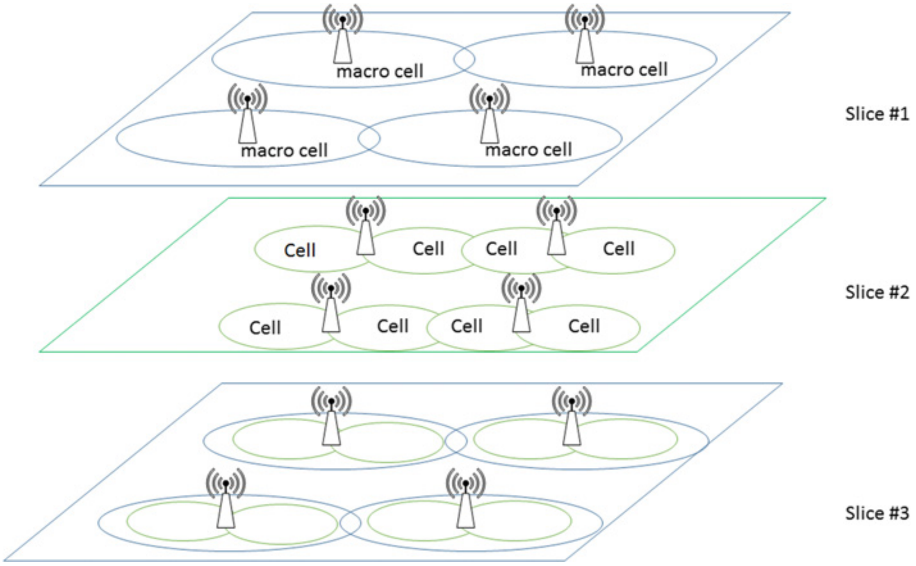

Fig. 3 Network slicing in RAN, based on [31]

erature. Many papers describe new slicing solutions and challenges, other refer to slicing survey. In paper [36], authors describe architectural requirements with reference to cloud-based 5G systems. Such a description implies RAN Layered Architecture based on the idea of network slicing. Moreover, authors consider influence of distributed memory concepts, VNF/VNA (Virtualized Network Function/Virtual Network Applications) idea, the dedicated data plane, and shared control plane as key areas of the future 5G network. Another solution considering RAN in 5G is described in paper [37]. It shows an approach to small cell which can be localized in edge cloud computing. The idea of small cell offers besides multi-operator radio access also growth in the capacity and the performance of existing RAN infrastructure. Authors claim that small cell should be considered in context of establishing E2E network slicing paradigm.

The authors of [38] present a new architecture for transport in 5G network. Proposed solution includes SDN/NFV-based management and orchestration (MANO) entity, Ethernet-based packet forwarding component and NFV-enabled processing entity. The goal of the concept is to fulfill QoS traffic requirements in 5G, especially in the network slicing idea.

The paper [39] refers to trends and prospects of leveraging SDN for the 5G networks. The document describes evolution of network from 3G to 5G, and the main 5G components: SDN, NFV, ICN (Information-Centric Networking), Mobile and Wireless Networks, Cooperative Cellular Networks and automatic QoS provisioning as elements are required to deploy this network.

4.2 Isolation and security

One of key expectations of network slicing is resources isolation. Each slice may be perceived as isolated set of resources configured through the network environment and providing defined set of functions. Level and strength of isolation may vary depending on slicing requirements and usage scenarios. At one scenario, there may be requirement for strict slices isolation, but in another, there may be required some communication between slices. Thus, isolation may be perceived in many ways, and it constitutes a set of properties chosen according to implementation needs. After analysis of 5G network slicing security issues [40, 41], the following isolation properties may be defined:

- Ring-fencing of each slice operational resources (e.g., storage, processor, operational memory), so that one slice cannot exhaust other slice's resources in any situation.
- Ring-fencing of resources for security protocols inside slice.
- Not supporting communication between slices (while ring-fencing resources concerns guarantee of minimal set of resources, this point concerns lack of information flow between two separate slices).
- Supporting communication between slices on strictly defined rules (like the previous point, it can be applied with complementary technique of ring-fencing of proper resources: operational and security).
- Cybersecurity assurance in the sense of protection against hacking one slice to influence another one.
- Signaling and management isolation to provide secure communication between slice and orchestrator as well as secure communication between elements inside a slice.
- Reliability assurance of different pieces of physical equipment used to span a slice.
- Secure communication between multiple network slice managers.
- Isolation concerning level of emission of information to slices' environment (e.g., side-channel attacks resistance).
- Isolation in hybrid environment including regular network functions (NFs) and virtualized NFs.
- Isolation of slices with one user equipment connected to multiple slices at a time.

Moreover, in [41] are described 5G-related security, trust and resilience problems and the advices how to overcome them. Not all properties should be implemented in each solution. There can be subsets of those properties chosen to meet specific requirements. Isolation may be achieved by different means, including [42]:

- Language-based isolation (type systems, certifying compilers);
- Sandbox-based isolation (Instruction Set Architecture, Application Binary Interface, Access Control List);
- Virtual machine (VM) based isolation (Process VM, Hypervisor VM, Hosted VM, Hardware VM);
- Operating system (OS) kernel based isolation;
- Hardware based isolation;
- Physical isolation.

Referring the above techniques of isolation to the slicing layers presented in Fig. 1 and to the network media interfaces, it can be noticed that language-based and sandbox-based techniques are especially suitable for providing isolation in service instance layer and network slice instance layer. The VM-based and OS kernel-based techniques are applicable at the network slice instance layer and the resource layer while hardware-based isolation and physical isolation can help in infrastructure/virtual infrastructure sharing among slices, especially at the interface RAN-CN, which is the hardest one for providing slices isolation.

Isolation-enabling means can be grouped using general categorization presented in the above list. Aside from this categorization, isolation assurance problem may be considered on network protocols level. There are several technologies enabling isolation of network resources, each one with its own characteristics and limitations. Below, there are listed example slices isolation enabling technologies:

- Tag-based network slices isolation such as MPLS (Multiprotocol Label Switching) uses special tags within packets to determine which slice they belong to.
- VLAN-based network slices isolation uses switch ports to partition the network on the second layer of OSI model.
- VPN-based network slices isolation uses special protocols such as IPSec, SSL/TLS (Secure Socket Layer/ Transport Layer Security, DTLS (Datagram Transport Layer Security), MPPE (Microsoft Point-to-Point Encryption), SSTP (Secure Socket Tunneling Protocol), SSH (Secure Shell) to provide authentication and confidentiality for transmission within each slice.
- SDN-based network slices isolation provides additional abstract layer to provide flexibility of slices management and is considered one of key enablers of 5G slicing [43].

To evaluate each of above technologies as well as other not listed, there is a need to define sets of common desired isolation properties and measures for those properties. Each set would represent specific business needs and description how to satisfy and measure them. A review of known communication protocols providing isolation on different security level can be found in [44].

4.3 SDN for network slicing

One of technologies mentioned above is SDN, which is considered as slicing enabler for core networks in 5G. It is a powerful tool that provides flexible services tailored to fit business needs. However, as a technology itself it carries also new attack vectors.

SDN security project [45] defines several areas of potential vulnerabilities including firmware abuse, eavesdropping, man-in-the-middle, APIs abuse, resource exhaustion, packet flooding, and more. Research [46] presents other attack vectors for SDN: misconfiguration of access to remotely accessible interfaces, malware infection at build time and runtime, and tenant attacks. As a response to these new threats, security assessment tools are being developed [47, 48]. Such tools and new attack vectors may be used to define desired isolation properties and measures. To satisfy properties selected for given slice configuration, there should be chosen suitable technologies working according to certain configuration and assumptions. One property can be satisfied by different technologies. Choice for suitable technology should be made according to optimization criteria for each case.

The paper [49] emphasizes that in 5G cellular networks virtualization and SDN are solutions which must handle data increase traveling form access and core network part. The SDN concept has some limitations in terms of planes separation among tenants and operators and lack of flexible capability to adapt to changing environment requirements. Therefore, some virtualization approaches do not ensure isolation of resources and do not guarantee bandwidth across the entities. These drawbacks are stopping the creation of slice network idea. Thus, SDN and virtualization solutions must realize the idea of 5G in which efficient resources allocation and multi-tenancy are required.

4.4 Isolation in wireless domain

In wireless domain, there are some techniques for slices isolation which are dedicated especially for this domain. This is due to special properties of air interfaces and medium. According to [25], there are the following strategies for resource isolation in 3GPP LTE and WiMAX:

- Physical resource block (PRB) scheduling;
- Slice scheduling;
- Traffic shaping.

For IEEE 802.11 (Wi-Fi) network there are similar strategies:

- EDCA (Enhanced Distributed Channel Access) control;
- Slice scheduling;
- Traffic shaping.

The following solutions can constitute an example of isolation techniques usage in wireless domain [25]:

- Virtual Basestation [50] in WiMAX implements isolation of slices with traffic shaping techniques in downlink.
- CellSlice [51] in WiMAX implements isolation of slices with slice scheduling and traffic shaping in uplink and sustained rate control in downlink.
- The papers [52] and [53] describe assigning resources in LTE with PRB scheduling in downlink.
- Virtual Wi-Fi [54] describes client virtualization in 802.11 networks using slice scheduling.

4.5 Management and orchestration

Network management is a fundamental function for establishment and functioning of the sliced network and for its security. The management starts with setting up slices and initiating communication in the sliced environment. Next, it manages slices and controls data transmission in a stable network state. Finally, it closes slices, performs accounting for transmission, and cleans aftereffects to prevent remainder attacks. Requirements and future expectations concerning management in sliced network are the subject of reference papers, public discussions, and research projects, see e.g., [55–57]. The papers presenting 5G management and orchestration, which is this part of management that can be automated, usually consider the ETSI NFV-MANO [58] as a reference model, see Fig. 4. ETSI NFV-MANO pretends to satisfy all expectations of future virtualized networks, including 5G. However, since it is very general, it needs additional specifications and clarifications. Some attempt of doing this is made by introducing additional standards specifying information flow at reference points (see [59]), but some of them are still draft standards, some other are under reconstruction, so the system is not complete. Since the ETSI NFV-MANO system is very general, it does not explicitly consider such real network problems like multi-tenancy, multi-vendor/multi-domain network's infrastructure and, what is the most important for security, it considers slicing isolation only on a basic level of performance isolation. Therefore, modifications and extensions of the management and orchestration system for 5G and virtualized networks are the subject of extensive studies.

One of possible improvements of ETSI NFV-MANO is joining it with SDN-like management, see, e.g., [60, 61]. The systems are compatible because they have plane-based/layered structure and both assume centralized management. Another extension tries to simplify management in multi-domain, multi-vendor, and multi-tenant systems by introducing hierarchical management and orchestration structures (see e.g., [23, 62–64]). Such an approach enables application of the ETSI NFV-MANO system directly for a single domain or instance and provide a supervision over several management systems. It also enables virtual functions and slice chaining in heterogeneous environment or when a slice is built over several domains, see e.g., [65–67].

Another aspect of management and orchestration in multi-domain networks has been considered in paper [68]. In such networks, each domain can work under different constraints (legal, technological, security, etc.). To establish a joint service (slice) over all domains, one must negotiate common conditions for all domains. This paper proposes using service-level agreement (SLA) criteria of orchestration. They are considered within the framework of orchestration model which represents a centralized approach assigned to a network's owner. However, in some specific networks (in our case: specific slices), e.g., Internet of Things systems, it is more suitable to apply a decentralized approach called a choreography (see e.g., [69]), where decision rules are negotiated among network elements according to their own interests.

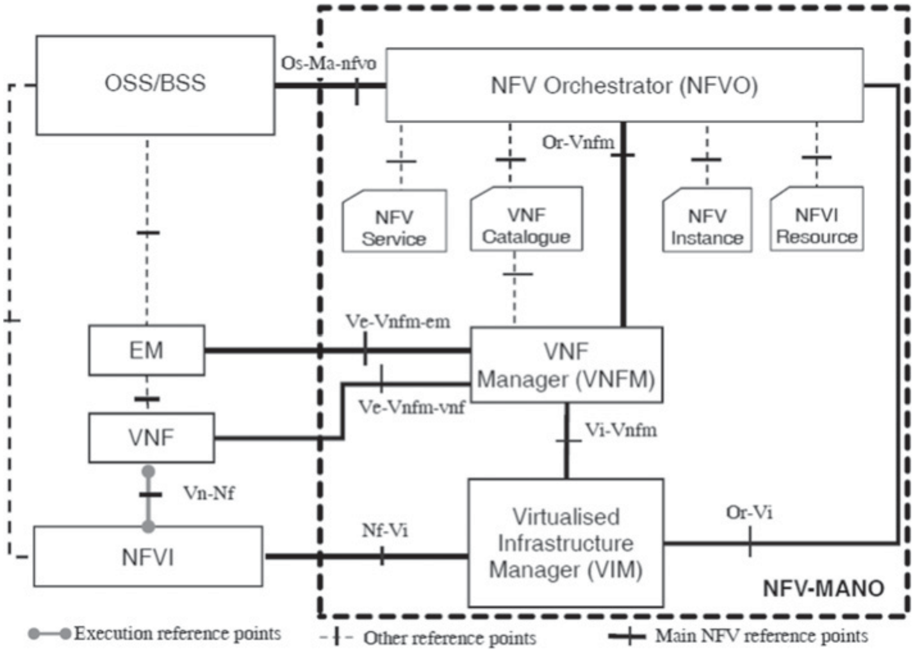

Fig. 4 The NFV-MANO architectural framework with reference points, [58]

Enhancing slicing property of the expected 5G networks led to extended ETSI NFV-MANO systems. Some approaches try to organize information flow in MANO (which is a critical and still unsolved problem) introducing it as a specific ETSI NFV-MANO service, see [70]. The other paper adds new orchestration functions dedicated specially to slicing, slicing in multi-tenant and multi-domain environments (see [71]). In addition to usual management and orchestration areas served by Virtual Infrastructure Manager, Virtual Network Function Manager and Network Functions Virtualization (NFV) Orchestrator, the authors have introduced a new element which is Inter-Slice Orchestrator and the highest orchestration element (NFVO) divided into two components: the slice orchestrator and the Service Orchestrator.

4.6 The transport problem

The crucial problem of network slicing is proper E2E connection. In a fixed part of the network, the slice could be defined in some network layer of the implemented stack of protocols. A node in the network can implement one or more of the following functionalities:

- The slice switch;
- The slice gateway;
- The slice multiplexer;
- The slice demultiplexer.

All these functionalities are assigned to links of slices. The slice switch and the slice gateway transport data from a source link to a target link (the relationship is $1to1$). The slice multiplexer and demultiplexer works on multiple links on one side (the $Nto1$ or $1toN$ relationship). It is not assumed here that source or target link(s) are from a single slice (the *slice chaining concept is allowed* described in [72], based on [73]). The slice's switch can combine two slice's links from the same layer in the common protocol stack. The slice gateway is slices' switch that can combine two slice's links from different layers or of different protocol stacks (or both). The slice multiplexer can merge multiple slices into a single slice, which could be later split up by a slice demultiplexer.

The data streams or the datagrams should be marked for switching/routing purposes: each of the mentioned devices must know how to handle incoming data. The mark could be, e.g., a MPLS label [74], the value of ToS field in the IPv4 protocol [75], or the flow label field in the IPv6 protocol [76]. In some scenarios, this functionality could be obtained by analyzing the source and destination IP addresses and transport layer's port numbers. The system should provide some mechanism for abuse detection. For multiplexing and demultiplexing purposes, the tunneling methods could be useful. The example of multiplexing property constitutes VPN connection, which links two distant networks using cryptographically secured tunnel through a third party network. Slices dedicated to different network services can be spanned from one linked network to another one using single VPN tunnel.

Multiplexing and demultiplexing do not require deep inspection on different layers of a slice. Data from different slices is marked; slices are grouped and sent through a common link. A switch and a gateway are more complicated according to slices analysis. In some cases, they would require accessing data sent through a slice to transfer it to the other slice. This means that such devices require special protection according to access to raw slices' data as well as a proper assurance for interconnecting slices, including preventing wrong interconnection of slices and potential data leakage.

5 Concerned issues in 5G networks

5G is an abbreviation for a future generation of telecommunications standards beyond the current wireless mobile 4G network. As such, the concept of 5G network faces new issues every day when already posed or identified tasks are solved. In this section, several problems which have been recently identified by prominent research groups and which stand for actual 5G issues are briefly presented.

On the web page of the IEEE SDN Technical Community, there is a white paper [77] presenting actual issues inspired by conditions resulting from techno-economic environment and policy constraints and proposing a change of paradigms in the design and operation of future telecommunications infrastructures dedicated to 5G networks. Main issues identified in the paper [77] are:

- Softwarization of the RAN, which is implemented as a C-RAN concept: the centralized, collaborative, clean, and Cloud Radio Access Network, resulting in new network's architecture, resources allocation, virtualization, SDN-like solutions, etc.
- An E2E vision for 5G, which should result in new service capabilities, interfaces, management and control schemes, access and non-access protocols with suitable procedures, functions, advanced algorithms, and new classes of virtual or physical resources.
- Application the Open Mobile Edge Cloud (OMEC), a functional node which will be deployed to provide seamless coverage and execute various control plane functions as well as some of the "core functions" currently placed in various nodes of the Evolved Packet Core (EPC).
- New solutions for planning, policy, and regulation resulting from different trust domains of virtualized functions and virtualized and non-virtualized infrastructure, which include:

  - The creation of a resilient policy;
  - The mapping and application of the policy to real hardware and software;
  - The visualization and enforcement of the policy, typically through visualization and enforcement tools.

- Provisioning of appropriately secure infrastructure (both, virtual and non-virtual).
- Management and maintenance of a deployment with multiple trust domains (which has been described in more detail in Section 4).
- Application of open source software as strategic for interoperability, innovations and research impacts, robustness and, consequently, network reliability and security.

The recent technical report [78] of the 3rd Generation Partnership Project (3GPP) concentrates on slicing as a crucial problem for development of 5G networks. It identifies several detailed key issues to be studied to provide and manage an isolated sliced environment for future networks. The basic questions in this area are:

- How to achieve isolation/separation between network slice instances and which levels and types of isolation/separation will be required?
- How and what type of resource and network function sharing can be used between network slice instances?
- How to enable a user equipment (UE) to simultaneously obtain services from one or more specific network slice instances of one operator?
- Which operations are crucial with regard to network slicing: network slice creation/composition, modification, deletion, etc.?
- Which network functions may be included in a specific network slice instance?
- Which network functions are independent of network slices?
- What are the procedures of choosing a network slice for the UE?
- How to support network slicing roaming scenarios?
- How to enable operators to use the network slicing concept to efficiently support multiple third parties (e.g., enterprises, service providers, content providers, etc.) that require similar network characteristics?

Future network expectations undergo different trends, visions, and requirements which must be considered to obtain effective, flexible, and reliable systems. Among them, the crucial are the following: heterogeneity in use cases, need to support different requirements from vertical markets, multi-vendor, and multi-tenant network models, etc. The method which could solve essential problems of 5G networks is slicing, in E2E slicing approach. Paper [79] addresses the key issues of how 5G devices may be enabled to discover, select, and access the most appropriate E2E network slices. Except for general requirements concerning E2E network slicing, the authors propose specific solution called Device Triggered Network Control mechanism. They define steps of the E2E slice selection and present results of simulations verifying usability of the mechanism proposed.

The authors in the article [80] list challenges and opportunities resulting from creating network slicing in 5G. Firstly, the paper describes concept of slicing: features, properties, and components. Then, a new 5G network slicing framework is considered. The framework includes three layers which contain a 5G software-defined infrastructure, virtual resources, applications and services, and a slicing management and orchestration (MANO). After the framework description, the authors propose seven challenges which should be investigated in future research. They are:

- Resource sharing;
- Dynamic slice creation and management;
- Isolation among network slices;
- Mobility management in network slicing;
- Security in network slicing;
- Wireless resource virtualization;
- Algorithmic aspects of resource allocation.

As it is seen, the proposed areas of investigation are essential for E2E secure network slicing, but they do not guarantee a complete solution of the problem.

The authors in [81] review the state of art in 5G network slicing. Moreover, they show a framework for discussing and evaluating existing work in a wide range. Finally, authors present a few areas which must be addressed when 5G network slicing is considered. As the most important are indicated:

- RAN virtualization;
- Service Composition with Fine-Grained Network Functions;
- End-to-end slice orchestration and management.

Such tasks are very general and consider only the component elements of an expected complete solution of the problem of secure E2E slice isolation in 5G networks.

The paper [82] gives a wide overview of 5G problems related to its architecture and applied modern virtualization concept. The authors identify several important slicing-related challenges, which are:

- Performance issues in a shared infrastructure;
- Management and orchestration issues;
- Security and privacy;
- New business models.

However, their considerations only partially cover E2E isolation problem.

The paper [83] concerns a centralized and dynamic approach to building network slices based on SDN. The solution enables to establish E2E slice, even to connect SDN and non-SDN devices to achieve multitenancy. Therefore, a special testbed has been developed to check the correctness of the discussed approach for dynamic E2E slice.

The overview studies related to providing E2E slices and slice isolation in future 5G networks presented in previous sections lead to some additional issues that extend the 3GPP considerations and focus them on E2E isolation approach. The E2E network slicing refers to a logical decomposition of the network instance layer including a specific character of network domain functions such as RAN or CN. In the E2E approach, slicing is associated with a term "slice chaining," which is an equivalent of the service chaining [27]. The service chaining is a technique for selecting and steering data flows using different kinds of service functions. Thus, the main idea is to choose proper resources of the network to establish connection with the required SLA level. In 5G approach, the slice chaining (see Fig. 5) is defined to establish one E2E connection through RAN and CN networks to a service provider.

Among many problems associated with the network slicing from the security point of view, the isolation of slice chaining is one of the most challenging. A flexible nature of the network slice should be characterized by a minimal influence on the services of this slice or other slices. Moreover, operators should assure the maximum amount of resources for every slice and their independence. Thus, the isolation of resources/slices should be provided. Section 6 presented several tasks and issues which should be addressed to provide E2E secure isolation in sliced network without unreasonable restricting the requirements of a network business model and network's technological constraints like accountability, sovereignty, performance, interoperability, etc.

6 Challenges for E2E slice isolation

In the paper [73], new challenges faced during establishment of E2E secure isolation of slices in 5G networks have been considered and briefly presented.

6.1 Providing standardized methods of design of isolated network slicing: patterns, parameters, technologies

Due to high diversity of each operator's network, the mechanisms, technologies, or configuration used for isolation of slices are going to be different in each case. To assure the proper quality of design for network slices isolation, there should be a developed framework covering requirements gathering and analysis. Such normalized approach would help network operators to consider the most important security issues and assure that common goals for network slicing are properly reached. One of the assumption of 5G is that slices must provide inter-slice isolation of sensitive data, approaching that of physically separated networks. To enable that, research in isolation domain should be performed.

5G must enable seamless inter-working of different network technologies, mobile, fixed, as well as satellite, potentially with different security levels (access control to 5G network) without jeopardizing the security level of each slices. In context of slicing, an isolation on a different level is required. One of the crucial issues is a definition of the isolation parameters. The isolation of the slices can be considered in at least four areas [84]:

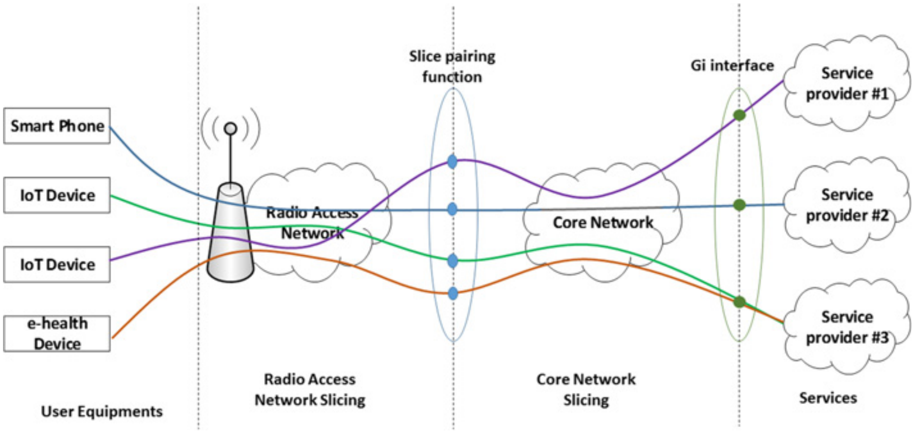

Fig. 5 The slice chaining concept, based on [72]

1. *Isolation of traffic*: all slices use the same network resources, so the network slices should ensure that data flow of one slice does not move to another.
2. *Isolation of bandwidth*: all slices allocate some bandwidth and should not utilize any bandwidth assigned to other slices. Thus, it is required to ensure the isolation of bandwidth on the links and nodes CPU, storage, or network capacity.
3. *Isolation of processing*: while all virtual slices use the same physical resources, a proper processing of packet is required, which will be independent of all other slices.
4. *Isolation of storage*: data related to a slice should be stored separately from data used by another slice.

Each area is marked by specific parameters which describe it. Even with knowledge about areas which should be isolated, there is nearly no information about parameters that need to be used to ensure the isolation. Some works associated with the isolation have been done within SDN concept but still they are far from being mature. In context of 5G network slicing such an approach is insufficient, as the isolation in 5G refers not only to SDN, but also to RAN.

A definition of parameters used in the isolation allows to create a methodology of their measurement. Based on that, it will be possible to determine their proper values. Finally, it will be helpful to check the isolation on the different levels. An unquestioned advantage of this methodology will be possibility to evaluate if isolation exists or not. The parameters of isolation have relations with others, so a set of their values and relations will be a literal proof of isolation existence.

Once a set of properties for slice is determined, proper technologies should be selected. There is a need to perform analysis of available slicing enabling technologies and then to determine potential security risks connected with each of the technology. Based on this risk analysis, there should be proposed countermeasures to minimize the risk. Technology can relate with protocols (e.g., OpenFlow as SDN protocol, routing protocols, cryptographic protocols), architecture paradigm (e.g., software-defined networking), implementations (e.g., SDN controller implementations, devices' firmware, operating systems) and hardware (e.g., used processors, Trusted Platform Modules, smart cards, USIM chips— Universal Subscriber Identity Module chips).

Further step in network slicing isolation design process is delivering proof of isolation on different levels of assurance. Once adequate isolation properties and technology are selected with respect to performed risk analysis, there is a need to define what kind of assurance a network operator would provide to his customers. There can be different levels of assurance from best effort to very strict security requirements, which would be defined during SLA agreement negotiations.

6.2 Secure E2E slice and inter-slice access and management

The 5G E2E approach to slicing brings additional complexity for slice and inter-slice access management. Two types of access procedures can be identified:

- Device selecting and attaching to the appropriate slice, cf. [79];
- Paring between RAN and CN.

Every entity of 5G network can have different access possibilities to different resources, due to specific requirements of every slice. For example, entities in the IoT network can have access to proper slices of IoT services, but access to e-health slices should be forbidden or restricted. The management of this access is very important in the context of proper slice creation. Lack of it causes security problems such as unauthorized access, which finally can be a reason of frauds.

Another aspect of this problem is mutual access between RAN and CN resources. A proper definition of paring functions is crucial when a slice is created: some RAN areas can establish connection with CN slices and some of them cannot. A proper management of the access to a slice is an important requirement to achieve a secure E2E path. Perhaps, properly applied C-RAN concept could be a remedy here.

In a sliced network, one also should consider services, which are connecting to ME (mobile equipment) via the slice that is specific for a given service. In such a case, ME must be able to receive traffic from RAN (considering 5G case), even if a slice instance used by this traffic has not been used before by this ME. Thus, one expects to have a protocol (governed by RAN or CN) that allows to attach securely a ME to the slice instance.

6.3 Support for method of providing access to common network functions shared between isolated slices

In network with slice isolation, there exists an unsolved problem of common network services and functions, like mobility management and AAA. It can be resolved for some services by adding a proxy server between an origin service and a user of services; each proxy should be assigned per slice. Proxies created for a single service could relate to each other (if number of them is relatively small) or managed by part of management layer (orchestration or choreography). This solution is suitable for cases without very strict constraints in the time domain, because in generic form, it requires solving the readers-writers' problem between slices related to the shared service or network function. Some of the operations can be handled in parallel (the read operations), but it depends on the context and internal implementation of the specific service. In other scenarios, the exclusive access to network function is necessary; it leads to situation where service client must wait in a queue for free time slot or client's request must be rejected by service, when the queue is full.

6.4 Providing a method of creation of new slices without violating current level of isolation between existing slices (especially in the 5G RAN)

Adding a new slice to currently established set of slice instances could cause some problems with satisfying QoS/QoE and isolation level in all slices. Even if resources are available, slices can affect each other. In the RAN, one can see this problem by interleaving communication channels in the frequency domain, which deteriorates SNR (signal-to-noise ratio) and consequently BER (bit error rate), throughput as well as causes packet loss, jitter, etc. Spread spectrum systems also have this problem, but in another way: the noise level increases with number of simultaneous transmissions which leads to similar complications. In the fibers, there is the FWM (four-wave mixing) problem: two different wavelengths produce two new unwanted wavelengths, which degenerate output signal from fiber. This effect can be minimized by properly chosen wavelength, but it limits the number of dynamically created isolated slices (apart from some other technical problems, like maximal number of waves handled by an optical terminal and non-zero distance between wavelength in grid).

Another practical problem is that each medium has some maximum available ratings like available throughput for all users, so always exists the maximum number of parallel users which use specific medium or resource. In the 5G network, this problem is generally more related to RAN than to the CN and this part should be optimized to avoid degradation of isolation by exhaustion of resources important for slices.

The isolation problem exists in RAN and CN simultaneously and should be considered in both parts of a network. However, in some scenarios, the CN part can be unused (i.e., a teleconference inside a single RAN cell), where all UEs are connected to one specific RAN part and E2E scenario does not need the CN to transport data.

The isolation problem can be considered over E2E approach (whole slice chain) or only over a single slice from slice chaining. Isolation in slice chaining should satisfy the rule that the isolation level of whole slice chain is not greater than the isolation level of any of slices inside the chain. The consequence of this rule is that network should first guarantee proper creation of slices inside each slice domain (RAN, CN, and other) and in next step an attempt to look after E2E slices' isolation. The slices in each domain can be created independently, but simultaneous creation could cause additional problems with isolation. The E2E slice could use slices created earlier if the slices' parameters are compatible (i.e., provided isolation level, throughput, availability).

The following solutions also can be considered: monitoring resources' utilization level and prevention of creating new slice instances if new instance harms QoS/QoE or isolation level; arranging slice instance reconciliation protocol which allows to change instances' requirements (might be, for a limited period).

6.5 Accounting and non-repudiation for slices' users and operators

While managing slices, there is always risk of unexpected events occurrence. Sometimes they are caused by hardware or software malfunction but also intended attacks may be performed involving one or more adversaries. In complex network environment with multi-vendor, multi-operator, and roaming support, it is hard to determine strict areas of responsibility for given incidents. It is important to deploy mechanisms able to point out in whose area of responsibility it is to deal with certain incidents and who is by law responsible for not holding proper isolation properties according to SLA.

Accounting relates to non-repudiation in such a way that non-repudiation provides evidence which prevents entity from denying of having performed given actions and thus enables accounting in accordance with those actions. Accounting and non-repudiation may be performed on different levels, beginning from single operator level in operator-operator and operator-customer relationships and finishing on single device in operator's network environment.

There are different means to reach non-repudiation using symmetric and asymmetric cryptography and proper trust relationships. The most commonly used techniques are based on Public Key Infrastructure (PKI) with digital certificates, but they are not always applicable, so there is a need to determine what kind of techniques can be used to provide accounting and non-repudiation in network slicing environment in general and specifically in 5G. Apart from strict hard security means like cryptography and security protocols, soft security methods, like trust relationships, have to be implemented in comprehensive solution. In PKI as an example, hard security is realized by asymmetric algorithms like RSA (Rivest-Shamir-Adleman algorithm) or ECDSA (Elliptic Curve Digital Signature Algorithm), used for certificate signing, while trust in certain Certificate Authority is a soft security.

In slicing environment, there is a need for gathering and utilizing evidence for certain actions and situations connected with users and operators. Further research should be done to develop architecture and mechanisms providing proper accounting and non-repudiation.

6.6 Design of MANO system suitable for a heterogeneous, dynamic, multi-vendor, and multi-tenant network

Concerning management and orchestration in the architectural framework for a multi-domain, multi-tenant isolated sliced environment, it has been reached the question if it should not be divided into several interconnected and hierarchic MANO subsystems concentrated on specific areas and periods of network functioning. They could be:

- Network management system;
    - For isolated slices establishment;
    - For isolated slices usage;
- Security management system including strong isolation establishment and checking.

The network management system for isolated slices establishment should cover, as a novel element, slices' chaining (also: services chaining within slices), as well as deciding which virtual service is exclusively assigned to a specific slice instance and which is shared. Network management system for isolated slices' usage must concentrate, except for usual network management, on assignment of users to specific slices and sharing competences among all actors involved: network providers, service providers, and end users. The security management system is crucial for strong slices isolation, and it must provide mechanisms for strong isolation establishment and permanent checking if isolation is not weakened or lost.

Another isolation problem which should be addressed in the context of network management is fulfillment of legal conditions related to telecommunication networks and network security. Such conditions can be different for various network domains (e.g., due to specific national regulations). Requirements on a lawful interception (LI) are a good example of such a problem. A solution could encompass including the legal conditions into Service Level Agreement requirements specific for each domain (or a network vendor) and then negotiating a common SLA for the whole slice. As a result, an operator can have sufficient access control delivered at slice level with end to end isolation (ciphering) in a way appropriate for all domains.

6.7 Unified interface and protocol for accessing the orchestrator

Services (service providers) and other networks should be treated in the same way from the orchestrator's perspective; also, common interface could be used here. Requests from other networks should have identified service source, so it is rational to handle this cases in the unified way. There should exists a negotiation protocol between orchestrators from different network operators which uses some slicing maintenance policy. The protocol should satisfy the following requirements:

- It should be fast enough, to be used during connection establishment between two or more endpoints,
- It should support energy-saving devices in simplified version of protocol (which could be a part of the entire protocol),
- The protocol should use authentication mechanisms to avoid abuse and attacks,
- It should allow to renegotiate currently established slices' parameters when it is required to satisfy new slice's set of requirements (i.e., KPIs—Key Product Indicators, QoS, QoE). The order in which slices should be included in renegotiation part should be defined in slicing maintenance policy,
- The protocol should allow to drop incoming API requests which are not authorized (if the authorization is required). It also should be resistant to DoS attacks,
- The API should share information about network's client only if the client had accepted that earlier. The client could be able to specify which services and networks can have access to information about him or her.

Sometimes new demands cannot be satisfied, even if the renegotiation has been used. This kind of situation also should be handled by maintenance policy. Demands could be queued in a priority queue; priority should depend on the type of demand source.

7 Types of isolation and isolation parameters

7.1 Isolation parameters

Isolation strength (measured or calculated) depends on various network and physical traits; some impact on isolation strength has software and hardware in use as well. There are considered two main types of traits:

- Enumerable trait, called property;
- Measurable trait, called parameter.

Another impact sources are metrics, introduced for RAN-sliced networks in [85], which are synthetic parameters, sometimes without easy network implementation. There are given examples of isolation properties (Table 1) and parameters (Table 2). Some traits can be considered both in the RAN and the CN; the rest of them are related to specific part of a network.

As it is stated in previous sections, isolation can be defined and analyzed using various properties and parameters; thus, overall isolation for each slice should be represented as a tuple of elements—parameters and properties.

Table 1 Examples of isolation properties

Isolation property
Used tunneling for traffic
Setting proper cryptographic primitives' (encryption, hashing, signing, etc.) parameters
Scalability (quantity of resources in O(n) notation)
Used user space virtualization technique (e.g., Docker [97] based on containers for applications)
Used network element virtualization technique (e.g., Kernel-based Virtual Machines [98] for virtual e-NodeB)
Mandatory access control
Inter-process communication (IPC)
Spectrum sharing techniques (e.g., TDMA, FDMA, OFDMA, CDMA - Time/ Frequency/Orthogonal Frequency/Code Division Multiple Access)
Location based isolation techniques (e.g., beamforming)
Physical elements separation (e.g., dedicated antennas)
Used layer 2 multiple access techniques and protocols with traffic isolation (e.g., CSMA/CA—carrier sense multiple access with collision avoidance)
Type of used band– licensed, partially licensed, unlicensed [99]
Hardware isolation method (e.g., separate e-NodeB hardware)
Sharing common link
Proper channel assignment for nodes in shared cell
Used VLAN tagging
Using SVIs (switched virtual interfaces)
Each VRF traffic is encapsulated inside a tunnel

Table 2 Examples of isolation parameters

Isolation parameter
Scheduling algorithms complexity
Maximum number of concurrent slices
Resilience to interception a single packet (datagram, frame)
Resilience to denial of service attacks (in attacking requests/s, attacks throughput)
Resilience to data injection
Static resilience to attacks against ring-fencing inter-slices
Static resilience to attacks against ring-fencing inside slice
Dynamic resilience to attacks against ring-fencing inter-slices
Dynamic resilience to attacks against ring-fencing inside a slice
Resilience for electromagnetic leaking (emanations)
Level of interferences between frequency channels (in signal's power terms)
Space division into sectors with sector antennas—ratio of covered space
by more than one antenna with significant power (i.e., up to 3 dB power loss) to whole space covered by antennas
Horizontal and vertical beamwidth for used antenna (in degrees)

Tuple's elements would vary depending on a business and technical goals for isolation analysis. Isolation can be defined as follows:

$$I = (a_1, a_2, ..., a_n)\,,$$

where:

- I is isolation parameters n-tuple,
- a_k is k-th property/parameter of isolation,
- n is the number of isolation parameters in each model.

Based on this definition, the proper models can be built to analyze isolation capabilities of different components of a network (e.g., switches, transmission cables, spectrum, specialized network nodes) as well as to define an E2E isolation as a function of isolation capabilities of each network component serving a slice.

7.2 Types of isolation

In network, multiplexing methods and access technologies are used widely, which divides and shares resources between channels. We can consider three main types of isolation for these methods:

1. *Full isolation*, when each channel has own part of available resources, e.g., time slots in TDMA;
2. *Partial isolation*, when channels can share part of available resources, e.g. channels in Wi-Fi;
3. *Zero isolation*, when all channels use some part of available resources, e.g. channels in OFDMA.

Generally, while using each method, we can observe some impact from another communication channels (i.e., from channels with another frequency band, signals using another code, echo signal generated with multi-path propagation [86, 87]), which usually changes in time. Signal propagation theory also describes important effects like attenuation [86, 87] and time dispersion [87] which can affect isolation level between signals.

In all these techniques, the isolation is provided by proper resource management. One can build multidimensional matrix (Fig. 6) with available resources and assign each cell to slice instance. However, in some applications, this naive algorithm will not work, i.e., IEEE 802.11b (Wi-Fi) wireless channels are very close to each other [88] and have significant effect on SNR (signal-to-noise ratio) and in consequences on available throughput (Fig. 7). In this case although Wi-Fi supports multiple channels, only few can be used simultaneously in one place. This solution provides method to avoid narrow-band interference from another device (i.e., microwaves), which can work in this unlicensed band at same time near the network equipment.

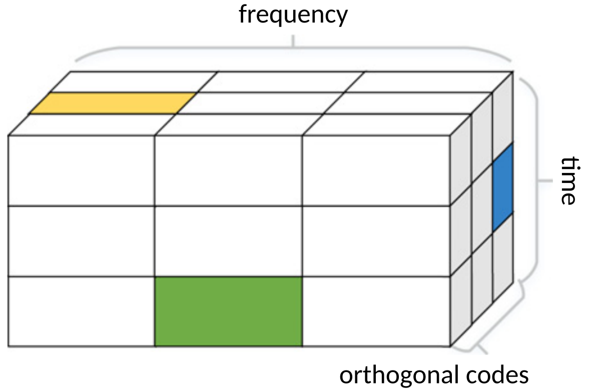

Fig. 6 Matrix with three resource dimensions and full isolation between communication channels

7.3 Service isolation

Isolation in slices could be considered as an isolation between services. The paper [89] has described a mathematical model of sliced network with services. In this model the separation relationship has been defined (marked as $f_{i,j}$ edges in the Fig. 8), which allows to consider the constraint which services (marked as nodes I_i) cannot share slice instance (marked as S_i nodes) during allocation of services to slices. The slice instance's ability to handle a service instance has been marked by edges between S and I nodes. Allocation should save resources and maximize income gained from supported services. Since the model uses integer programming method, for practical use, the heuristic algorithm has been proposed which solves proposed optimization problem.

8 Isolated slicing management and orchestration

All management and orchestration schemes presented above, both the ETSI NFV-MANO and extended models, consider the network as a sliced medium with slices isolation on a level of performance isolation, which is natural in 5G slices concept. For a stronger, secure (cryptographic) isolation, a new orchestration aspect should be considered, which is secure isolated slice establishment at the slices establishment stage, and isolation checking at the second, network exploiting stage. Finally, when the slice is being closed, secure critical data destruction must be performed to prevent post-dated loose of isolation. Thus, a new management and orchestration scheme must be proposed, where isolation establishment at each stage of a slice lifetime is considered. The scheme must consider also such elements as slice chaining, isolation establishment, and isolation checking and monitoring. A draft proposal of such a new extended scheme is in Fig. 9, where the revised ETSI NFV-MANO architectural framework for a multi-domain, multi-tenant isolated sliced environment is presented.

Management algorithms could have different resilience against ring-fencing attacks (or overusing the network) and side effect of this is providing different strength of isolation, especially in terms of static and dynamic resilience against the ring-fencing (listed in Subsection 7.1). The static resilience is defined as the ability of network to handle more traffic (or services) at some network state. The dynamic resilience is the ability to return to satisfying the QoS requirements after fast and big increase of offered traffic (or services) in network. The change of traffic for measuring the dynamic resilience should be like the Heaviside step function; for the static resilience should be slower than time required by management protocols to rearrange resources between slices.

Concerning possible attacks on 5G networks and suitable countermeasures, a great advantage is application of the SDN methodology in network management. Such an approach makes possible integration of active protection methods (distributed firewalls and Intrusion

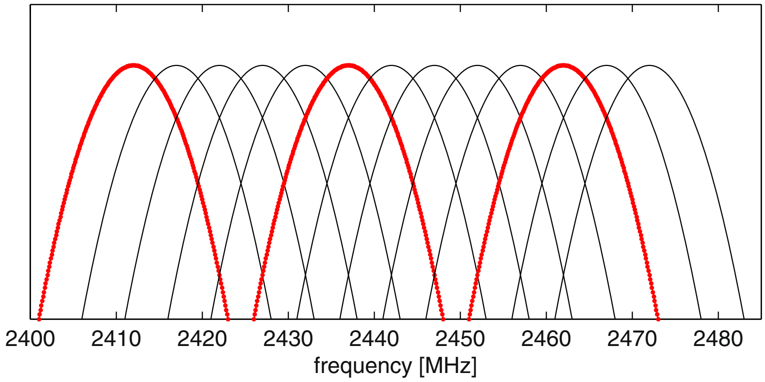

Fig. 7 Example of partial isolation which exists in IEEE 802.11b (ETSI regulatory domain; based on [88]). Each parabola shows range of single channels band. Red marked channels are pairs isolated, but another pairs (i.e., two left most channels) are not

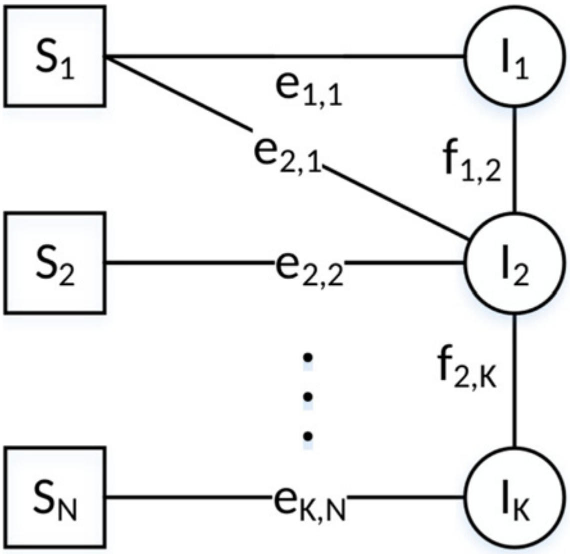

Fig. 8 Graph model of slice instances and service instances described in [89]. Image based on [89]

Detection/Prevention Systems) into the MANO, see e.g., [90]. Successful integration of the active security elements with the 5G management system is the crucial element of its usability for E2E isolated slicing.

The analysis of requirements and constraints appearing in such a complicated environment proves that every MANO system trying to reflect all aspects of reality would be completely nonfunctional and too complex to be implemented and controlled. The question is, should it be considered as a single management and orchestration system or is it better to divide it into several cooperating and interdependent/hierarchic MANO subsystems? This proposal should be further analyzed to outline frames of each MANO subsystem and to integrate them. Such an approach restricts the number of required information flow specifications on MANO interfaces (where not all are defined yet) and introduces several information flows between MANO subsystems to be specified.

Management and orchestration reflect all problems connected with, both, network establishment and network every day functioning. The sections above have tried to reflect basic issues connected not only with MANO, but also with 5G functioning, which are already identified and at least partially solved. However, E2E security still requires special attention and deep studies. In the following sections, there are presented several challenges faced while trying to construct a slice which is effective from technological and business point of view and which additionally could provide E2E security for an end-user or a service provider.

An immanent part of the 5G management system is its area related to security [91]. Since 5G network concept is under construction, one can propose the most sophisticated security measures to provide its security. For instance, the report [92] gives arguments why security is fundamental to 5G, and how it is different from earlier generation network security in relation to requirements, threat landscape, and possible solutions. Probably the most complete specification of security management problem in 5G is given in the white paper [93]. Among other problems, the report appreciates the role of lightweight security measures which usually include trust establishment between network entities, trust management, and using entities' reputation for long-term recommendations via application of reputation systems. In some cases, using reputation can even support quick network

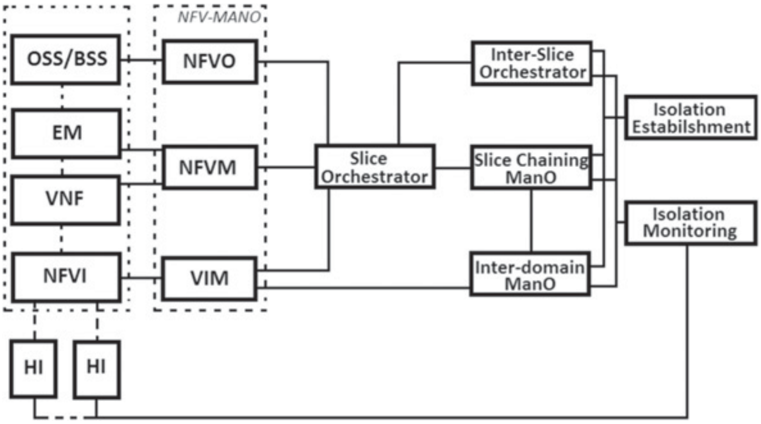

Fig. 9 The extended NFV-MANO architectural framework for isolated sliced environment (OSS/BSS - Operations Support System/Business Support System; EM - Element Manager; VNF - Virtual Network Function; NFVI - Network Functions Virtualization Infrastructure; HI - Hardware Infrastructure; NFVO - Network Functions Virtualization (NFV) Orchestrator; NFVM - NFV Manager, VIM Virtual Infrastructure Manager)

management decisions. For instance, in [94] it has been shown that reputation-based support in dynamic environment could improve routing decisions affecting positively the QoS level stability, what also in 5G isolated slicing is very important. Reputation management systems could also improve security level of the network working as a lightweight firewall solution giving long-term recommendation for acceptance of network's resources activity, see [95].

Another interesting area of application of trust and reputation management in 5G networks is including it into security enabler that can be applied to improve the network's own security and utilized by network users in their own service protection methods. To provide this functionality, the Network Provided Trustworthiness (NPT) system matching 5G architecture has been proposed and analyzed in the paper [96]. The main role of this system is to offer security context describing each connection that allows to take trust decisions. To build such security context, relevant information needs to be collected at each segment of the network. Finally, it should be aggregated, correlated, and propagated to provide trustworthiness information for future decisions regarding security, fraud prevention, or characterization of risk.

In the 5G network architecture trustworthiness enabler functionality can be achieved with specialized subsystem distributed over the network. As depicted in Fig. 10, dedicated agents Trustworthiness Watchers (TW) need to be placed in subsystems of 5G network, where information about connection is generated or processed. In the presented 5G ecosystem, TW agents are present in network infrastructure (both physical and virtual), network functions, and service layers both in access and core networks. Another set of information can be extracted from management systems and end to end (E2E) orchestration layer.

Native network information received from TWs is aggregated and correlated by NPT system. The resultant trustworthiness information can be made available to network operator's service platforms or third party platforms offering services over the network in the form of security context. Dynamic and programmable nature of 5G network allows not only computation of trustworthiness information but also negotiation and enforcement of required trustworthiness level.

With NPT system, isolated slicing management is facilitated by indicating trustworthiness of each component of access and core network. Trustworthiness information computed by NPT reflects the security level of each component. The slice security policy can state weather this level is high enough; the given (physical or real) component can be included in the slice. Using trustworthiness information, the security level can be continuously monitored over the lifetime of the slice.

9 Conclusions

As it has been mentioned in this paper, there are many projects connected with researches in an area of 5G. The wide range of them indicate the complexity of the issue. Potentially, the results of research will develop the 5G architecture leading it to a mature state, so it is important to investigate this new concept in a detailed way. In this paper, an attempt to reconsider the concept of secure slicing in a realistic ecosystem of heterogeneous multi-vendor multi-tenant 5G network has been made. In such a network, to assure E2E isolation on a certain strength level and to introduce adequate security policy, it is necessary to identify isolation attributes and to create a kind of abstraction layer. Properly defined attributes are the basis to determine the E2E level of isolation. It is the way which allows the user to define, deploy, and adapt (if necessary) security policies accordingly to the expectations and service protection needs. Consideration of resource description in 5G networks leads to conclusion that currently there is no common description of isolation capabilities that could be used for automatic deployment. To define an abstraction for different resources, it is necessary to specify attributes allowing unambiguous definition and rigorous verification of isolation level in each slice. It is important to define expected initial isolation level (e.g., performance isolation) as well as to design mechanisms for dynamic isolation improvement for a given service. Dynamic isolation mechanism should be also able to create isolated resources with proper capabilities or to address inter-slicing communication to use virtual resources from a different slice in the way that will not breach global security policy rules.

To make the general idea presented above applicable in practice, it has been decided to formulate detailed issues which cover partial tasks leading to the complete solution. The tasks set out in this paper as well as the analysis which precedes it are the result of extensive state-of-the-art studies on network slicing and network sovereignty and discussions held between research groups of Orange Labs and Warsaw University of Technology. Proposed tasks, although they cover a wide range of issues related to isolated network slicing, do not cover all important areas for slice isolation. The areas related to communication hardware-based technologies have been deliberately skipped, while concentrating on those solutions which are management-related and which are expected to be software-based.

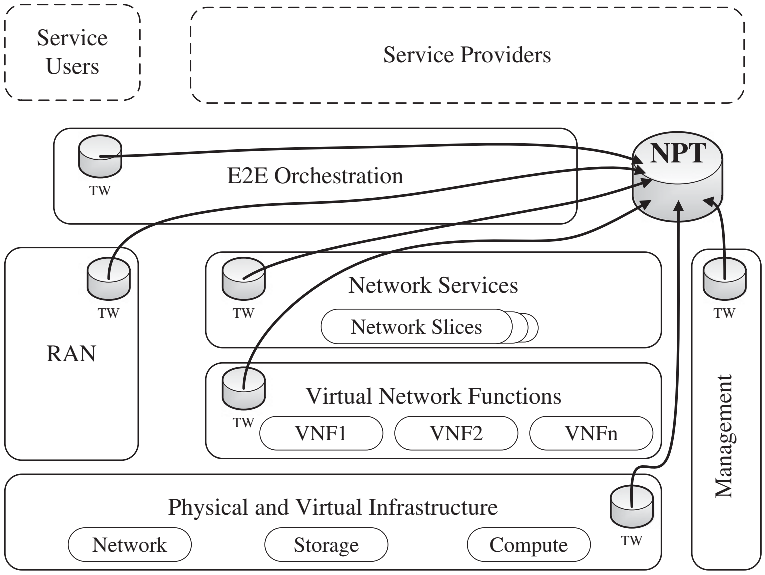

Fig. 10 NPT system within 5G ecosystem: logical view

The next steps of the research are the following: filling the draft frameworks presented above with hard principles and structural elements along with their interdependencies, estimating expected parameters, and verifying experimentally functionality of the resultant isolated slices model. To initiate such a research, this paper has presented the outline of isolation types and isolation parameters problems. Moreover, several main tasks of an isolated-slicing-dedicated MANO system have been pointed out.

There are many challenges to be addressed in the topic presented in this paper. In the authors' opinion, the research in the following areas (divided into two main parts) would constitute a step forward in E2E slice isolation:

- The network slicing area:
  - Preparing mechanisms for slices interconnection to provide E2E slicing in dynamic heterogeneous systems with multiple tenants;
  - Development of secure management of slices creation, modification, and deletion;
  - Enabling accounting for slices' users and ensuring non-repudiated access to slices.
- The slice isolation area:
  - Designing formal methods to proof isolation properties of an E2E slice;
  - Proposing new isolation models and numerical analysis of isolation properties in E2E slice to observe the isolation in actual network state;
  - Enabling secure network functions sharing between slices.

The first area focuses on the management part of the network slicing problem in the E2E aspect. The second area considers network slicing from a need of isolation point of view. The isolation-oriented approach merges knowledge from different branches, e.g., classical security methods approach, new soft-security methods, like trustworthiness and reputation systems, or QoS/QoE-related issues. In the authors' opinion, both areas are very important and should be subject of further research.

Abbreviations

3GPP: 3rd generation partnership project; 5G: Fifth generation telephony; 5G PPP: 5G infrastructure public-private partnership; AAA: Authentication, authorization, accounting; API: Application programming interface; BER: Bit error rate; CHARISMA: Converged heterogeneous advanced 5G cloud-ran architecture for intelligent and secure media access; CDMA: Code division multiple access; CN: Core network; C-Plane/U-Plane: Control plane/user plane; CSMA/CA: Carrier sense multiple access with collision avoidance; DoS: Denial of service; DTLS: Datagram transport layer security; E2E: End-to-end; ECDSA: Elliptic curve digital signature algorithm; EPC: Evolved packet core; ETSI: European telecommunications standards institute; FWM: Four-wave mixing; ICN: Information-centric networking; IEEE: Institute of Electrical and Electronics Engineers; IoT: Internet of Things; IPv4/IPv6: Internet protocol version 4/6; ITU: International Telecommunication Union; IPSec: Internet Protocol Security; KPI: Key product indicator; LI: Lawful interception; LTE: Long term evolution; MAC: Medium access control; MANO: Management and orchestration architecture; ME: Mobile equipment; MPLS: Multiprotocol label switching; MPPE: Microsoft point-to-point encryption; NFV: Network function virtualization; NOMA: Non-orthogonal multiple access; NPT: Network provided trustworthiness; (O)FDMA: (Orthogonal) frequency division multiple access; OMEC: Open mobile edge cloud; OS: Operating system; OSI: (ISO) open systems interconnection (reference model); PHY layer: Physical layer; PKI: Public key infrastructure; PLS: Physical layer security; PRB: Physical resource block; QoE/QoS: Quality of experience/quality of service; RAN: Radio access network; RAT: Radio access type; RSA: Rivest-Shamir-Adleman algorithm; SDN: Software defined network; SLA: Service level agreement; SNR: Signal to noise ratio;

SSH: Secure shell; SSL/TLS: Secure socket layer/transport layer security; SSTP: Secure socket tunneling protocol; SVI: Switched virtual interface; TDMA: Time division multiple access; TW: Trustworthiness watcher; UE: User equipment; USIM: Universal subscriber identity module; VLAN: Virtual LAN; VM: Virtual machine; VNA: Virtual network applications; (V)NF: (Virtualized) network function; VPN: Virtual private network

Funding
Not applicable.

Availability of data and materials
Not applicable.

Authors' contributions
All authors actively participated in discussions and studies which resulted in this paper. All authors read and approved the final manuscript.

Competing interests
The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details
[1]Institute of Telecommunications of WUT, Nowowiejska 15/19, 00-665 Warsaw, Poland. [2]Orange Polska S.A., Warsaw, Poland. [3]Orange Labs, Paris, France.

Received: 20 November 2017 Accepted: 5 March 2018
Published online: 20 March 2018

References

1. 5G-PPP . https://5g-ppp.eu/. Accessed 12 Mar 2018
2. CHARISMA. http://www.charisma5g.eu/. Accessed 12 Mar 2018
3. 5G ENSURE. www.5gensure.eu. Accessed 12 Mar 2018
4. 5G NORMA. http://www.it.uc3m.es/wnl/5gnorma/pdf/5g_norma_d4-1.pdf. Accessed 12 Mar 2018
5. 5G Crosshaul. http://5g-crosshaul.eu/wp-content/uploads/2018/01/5G-CROSSHAUL_D1.1.pdf. Accessed 12 Mar 2018
6. 5GEx. http://www.5gex.eu/. Accessed 12 Mar 2018
7. METIS-II. https://metis-ii.5g-ppp.eu/. Accessed 12 Mar 2018
8. Flex5Gware. http://www.flex5gware.eu/. Accessed 12 Mar 2018
9. SliceNet. https://slicenet.eu/. Accessed 12 Mar 2018
10. 5G ESSENCE. www.5g-essence-h2020.eu/. Accessed 12 Mar 2018
11. 5G-MoNArch. https://5g-monarch.eu. Accessed 12 Mar 2018
12. Matilda. http://www.matilda-5g.eu. Accessed 12 Mar 2018
13. 5G!PAGODA. https://5g-pagoda.aalto.fi/. Accessed 12 Mar 2018
14. S Kuklinski, T Osinski, L Tomaszewski, A Ksentini, E Cau, M Corici, in *2017 European Conference on Networks and Communications (EuCNC), Poster Sesion 1*. A flexible approach to mobile network slicing: 5G!Pagoda vision (EuCNC, Oulu, 2017
15. FG IMT-2020. https://www.itu.int/en/ITU-T/focusgroups/imt-2020/Pages/default.aspx. Accessed 12 Mar 2018
16. TS 23.501 System Architecture for the 5G System, Release 15 (2017). 3GPP Portal. http://portal.3gpp.org/
17. TS 23.502 Procedures for the 5G System, Release 15 (2017). 3GPP Portal. http://portal.3gpp.org/
18. TS 23.503 Policy and Charging Control Framework for the 5G System; Stage 2, Release 15, (2017). 3GPP Portal. http://portal.3gpp.org/
19. Dynamic end-to-end network slicing for 5G, Nokia White Paper (2016). Global mobile Suppliers Association. https://gsacom.com
20. T Shimojo, Y Takano, A Khan, S Kaptchouang, M Tamura, SH Iwashina, in *Proc.1st IEEE Conference on Network Softwarization (NetSoft)*. Future mobile core network for efficient service operation, (2015), pp. 1–6. https://doi.org/10.1109/NETSOFT.2015.7116190
21. U Herzog, A Georgakopoulos, I-P Belikaidis, P Demestichas, S Diaz, Ó Carrasco, F Miatton, K Moessner, V Frascolla, Quality of service provision and capacity expansion through extended-DSA for 5G.Trans. Emerg. Telecommun. Technol. **27**(9), 1250–1261 (2016). https://doi.org/10.1109/EuCNC.2016.7561032
22. A Nakao, P Du, Y Kiriha, F Granelli, AA Gebremariam, T Taleb, M Bagaa, End-to-end network slicing for 5G mobile networks. J. Inf. Process. **25**, 153–163 (2017). https://doi.org/10.2197/ipsjjip.25.153
23. View on 5G Architecture, 5G PPP Arch. Working Group (2016). https://5g-ppp.eu/
24. O Bulakci, Towards Sustainable 5G Networks [PDF slides] (2015). Retrieved from http://www.ieeevtc.org/conf-admin/vtc2015fall/15.pdf
25. M Richart, J Baliosian, J Serrat, J-L Gorricho, Resource slicing in virtual wireless networks: a survey. IEEE Trans. Netw. Serv. Manag. **13**(3), 462–476 (2016). https://doi.org/10.1109/TNSM.2016.2597295
26. PA Abdulla, J Cedergerg, L Kaati, in *Proc. 4th Int. Symp. Leveraging Applications, ISoLA 2010*. Analyzing the security in the GSM radio network using attack jungles, (Greece, 2010), pp. 60–74. https://doi.org/10.1007/978-3-642-16558-0_8
27. T Yoo, in *7th Int. Conf. Information and Communication Technology Convergence*. Network slicing architecture for 5G network (IEEE, Korea, 2016), pp. 1010–1014. https://doi.org/10.1109/ICTC.2016.7763354
28. Z Ma, ZQ Zhang, ZG Ding, PZ Fan, HCH Li, Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives. Sci. China Inf. Sci. **58**(4) (2015). https://doi.org/10.1007/s11432-015-5293-y
29. L Peterson, T Anderson, D Culler, T Roscoe, A blueprint for introducing disruptive technology into the Internet. ACM SIGCOMM Comput. Commun. Rev. **33**(1), 59–64 (2003). https://doi.org/10.1145/774763.774772
30. P Hedman, Description of Network Slicing Concept (NGMN Alliance, 2016). https://www.ngmn.org/fileadmin/user_upload/160113_Network_Slicing_v1_0.pdf
31. Q Li, G Wu, A Papathanassiou, L Wei, in *Proc.ETSI Workshop on Future Radio Technologies and Air Interfaces*. End-to-end network slicing in 5G wireless communication systems, (2016), pp. 1–4. https://docbox.etsi.org/Workshop/2016/201601_FUTURERADIOTECHNOL_WORKSHOP/S06_ADVANCED_TOPIC_FUTURE_AIR_INTERFACES/END2END_NWK_SLICING_5G_WIRELESS_COMM_SYSTEMS_paper.pdf
32. Q Li, G Wu, A Papathanassiou, U Mukherjee, An end-to-end network slicing framework for 5G wireless communication systems (2016). arXiv:1608.00572 [cs.NI]
33. 5G Americas White Paper: Network Slicing for 5G and Beyond (2016). www.5gamericas.org
34. X Foukas, MK Marina, K Kontovasilis, in *The 23rd Annual International Conference on Mobile Computing and Networking (MobiCom'17)*. Orion: RAN Slicing for a Flexible and Cost-Effective Multi-Service Mobile Network Architecture, (2017), pp. 127–140. https://doi.org/10.1145/3X00000.117811.3117831
35. Ericsson: A vision of the 5G core: flexibility for new business opportunities, (2016). https://www.ericsson.com/en/ericsson-technology-review/archive/2016/a-vision-of-the-5gcore-flexibility-for-new-business-opportunities
36. K Katsalis, N Nikaein, E Schiller, R Favraud, TI Braun, in *2016 IEEE International Conference on Communications Workshops (ICC)*. 5G architectural design patterns, (2016), pp. 32–37. https://doi.org/10.1109/ICCW.2016.7503760
37. IP Chochliouros, Giannoulakis I, AS Spiliopoulou, M Belesioti, A Kostopoulos, E Sfakianakis, A Kourtis, E Kafetzakis, S Agapiou, in *CSCC 2017 MATEC Web of Conferences*. A novel architectural concept for enhanced 5G network facilities, vol. 125, (2017), p. 03012. https://doi.org/10.1051/matecconf/201712503012
38. X Costa-Perez, A Garcia-Saavedra, X Li, T Deiss, A de la Oliva, A di Giglio, P Iovanna, A Moored, 5G-Crosshaul: An SDN/NFV integrated Fronthaul/Backhaul transport network architecture. IEEE Wirel. Commun. **24**(1), 38–45 (2017). https://doi.org/10.1109/MWC.2017.1600181WC
39. A Hakiri, P Berthou, Leveraging SDN for the 5G networks: trends, prospects and challenges (2015). https://arxiv.org/abs/1506.02876. Accessed 12 Mar 2018
40. R Harel, S Babbage, *5G security recommendations Package 2: Network Slicing*. (NGMN Alliance, 2016). https://www.ngmn.org/fileadmin/user_upload/160429_NGMN_5G_Security_Network_Slicing_v1_0.pdf
41. G Arfaoui, JMS Vilchez, J-P Wary, in *IEEE Trustcom/BigDataSE/ICESS*. Security and resilience in 5G: current challenges and future directions, (Sydney, 2017), pp. 1010–1015. https://doi.org/10.1109/Trustcom/BigDataSE/ICESS.2017.345

42. A Viswanathan, BC Neuman, A survey of isolation techniques. Univ. South. Calif. Inf. Sc. Ins., 1–16 (2009). preprint, http://www.arunviswanathan.com/content/pdfs/survey_isolation_techniquesv2.pdf
43. Applying SDN Architecture to 5G Slicing, Open Networking Foundation (2016). https://www.opennetworking.org
44. V Del Piccolo, A Amamou, K Haddadou, G Pujolle, A survey of network isolation solutions for multi-tenant data centers. IEEE Comm. Surv. Tutorials. **18**(4), 2787–2821 (2016). https://doi.org/10.1109/COMST.2016.2556979
45. SDN security project. http://www.sdnsecurity.org/. Accessed 12 Mar 2018
46. CH Yoon, S Lee, *Attacking SDN Infrastructure: Are, We Ready for the Next-Gen Networking?* (BlackHat, 2016). https://www.slideshare.net/cisoplatform7/attacking-sdn-infrastructure-are-we-ready-for-the-next-gen-networking
47. DELTA: A Penetration Testing Framework for Software-Defined Networks, Open Networking Foundation (2016). https://www.slideshare.net/cisoplatform7/attacking-sdn-infrastructure-are-we-ready-forthe-next-gen-networking
48. S Lee, J Kim, S Shin, P Porras, V Yegneswaran, in *47th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*. Athena: a framework for scalable anomaly detection in software-defined networks, (2017), pp. 249–260. https://doi.org/10.1109/DSN.2017.42
49. CH Tsirakis, P Matzoros, G Agapiou, in *CSCC 2017 MATEC Web of Conferences*. State-of-the-art on virtualization and software defined networking for efficient resource allocation on multi-tenant 5G networks, vol. 125, (2017), p. 03009. https://doi.org/10.1051/matecconf/201712503009
50. G Bhanage, I Seskar, R Mahindra, D Raychaudhuri, in *Proc. 2nd ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures*. Virtual basestation: architecture for an open shared WiMax framework (ACM, 2010), pp. 1–8. https://doi.org/10.1145/1X00000.851399.1851401
51. R Kokku, R Mahindra, Zhang H, S Rangarajan, in *5th Int. Conf. Communication Systems and Networks (COMSNETS)*. Cellslice: Cellular wireless resource slicing for active RAN sharing (IEEE, 2013), pp. 1–10. https://doi.org/10.1109/COMSNETS.2013.6465548
52. Y Zaki, L Zhao, C Goerg, A Timm-Giel, in *3rd Joint IFIP Wireless and Mobile Networking Conf. (WMNC)*. LTE wireless virtualization and spectrum management (IEEE, 2010), pp. 1–6. https://doi.org/10.1109/WMNC.2010.5678740
53. Y Zaki, L Zhao, C Goerg, A Timm-Giel, LTE mobile network virtualization. Mob. Netw. Appl. **16**(4), 424–432 (2011). https://doi.org/10.1007/s11036-011-0321-7
54. L Xia, S Kumar, X Yang, P Gopalakrishnan, Y Liu, S Schoenberg, X Guo, Virtual wifi: bring virtualization from wired to wireless. ACM SIGPLAN Not. **46**(7), 181–192 (2011). https://doi.org/10.1145/1X00000.952682.1952706
55. Network Functions Virtualisation (NFV). Network Operator Perspectives on Industry Progress, ETSI NFV Whitepaper 3 (2014). https://https://portal.etsi.org/Portals/0/TBpages/NFV/Docs/NFV_White_Paper3.pdf
56. HJ Son, CH Yoo, E2E Network Slicing Key 5G technology : What is it? Why do we need it? How do we implement it? Netmanias Web Page (2015). https://www.netmanias.com/en/post/blog/8325/
57. The 5G Infrastructure Public Private Partnership web page. https://5g-ppp.eu/. Accessed 12 Mar 2018
58. ETSI GS NFV-IFA 009 V1.1.1 (2016-07) Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options. http://www.etsi.org/deliver/etsi_gs/NFV-IFA/001_099/009/01.01.01_60/gs_NFV-IFA009v010101p.pdf
59. ETSI NFV standards web page. http://www.etsi.org/technologies-clusters/technologies/nfv/. Accessed 12 Mar 2018
60. R Nejabati, S Peng, M Channegowda, B Guo, D Simeonidou, SDN and NFV convergence a technology enabler for abstracting and virtualising hardware and control of optical networks. Opt. Fiber Comm. Conf. and Exhib. (OFC) (2015). https://doi.org/10.1364/ofc.2015.w4j.6
61. R Munoz, R Vilalta, R Casellas, R Martinez, T Szyrkowiec, A Autenrieth, V Lopez, D Lopez, Integrated SDN/NFV management and orchestration architecture for dynamic deployment of virtual SDN control instances for virtual tenant networks. J. Opt. Comm. Netw. **7**(11), B62–B70 (2015). https://doi.org/10.1364/jocn.7.000b62
62. LM Contreras, CJ Bernardos, A de la Oliva, X Costa-Perez, R Guerzoni, in *Eur. Conf. Networks and Comm. (EuCNC)*. Orchestration of crosshaul slices from federated administrative domains, (Athens, 2016), pp. 220–224. https://doi.org/10.1109/eucnc.2016.7561036
63. X Zhou, R Li, T Chen, H Zhang, Network slicing as a service: enabling enterprises' own software-defined cellular networks. IEEE Commun. Mag. **54**(7), 146–153 (2016). https://doi.org/10.1109/mcom.2016.7509393
64. P Rost, A Banchs, I Berberana, M Breitbach, M Doll, H Droste, C Mannweiler, MA Puente, K Samdanis, B Sayadi, Mobile network architecture evolution toward 5G. IEEE Commun. Mag. **54**(5), 84–91 (2016). https://doi.org/10.1109/mcom.2016.7470940
65. H Moens, F De Turck, Customizable function chains: managing service chain variability in hybrid NFV networks. IEEE Trans. Netw. Serv. Manag. **13**(4), 711–724 (2016). https://doi.org/10.1109/tnsm.2016.2580668
66. J Halpern, C Pignataro, in *RFC 7665*. Service function chaining (SFC) architecture (IETF, 2015). https://doi.org/10.17487/rfc7665
67. F Bari, SR Chowdhury, R Ahmed, R Boutaba, OCMB Duarte, Orchestrating virtualized network functions. IEEE Trans. Netw. Serv. Manag. **13**(4), 725–739 (2016). https://doi.org/10.1109/tnsm.2016.2569020
68. A Stanik, M Koerner, O Kao, Service-level agreement aggregation for quality of service-aware federated cloud networking. IET Netw. **4**(5), 264–269 (2015). https://doi.org/10.1049/iet-net.2014.0104
69. S Cherrier, YM Ghamri-Doudane, S Lohier, G Roussel, in *IEEE World Forum on Internet of Things (WF-IoT)*. Fault-recovery and coherence in internet of things choreographies, (Seoul, 2014), pp. 532–537. https://doi.org/10.1109/wf-iot.2014.6803224
70. L Mamatas, S Clayman, A Galis, Information exchange management as a service for network function virtualization environments. IEEE Trans. Netw. Serv. Manag. **13**(3), 564–577 (2016). https://doi.org/10.1109/TNSM.2016.2587664
71. Functional Network Architecture and Security Requirements. 5G-NORMA Deliverable D3.1. http://www.it.uc3m.es/wnl/5gnorma/pdf/5g_norma_d3-1.pdf
72. 5G systems - Enabling industry and society transformation, Ericsson White Paper, UEN 284 23-3244, 2015. https://www.ericsson.com/en/white-papers/5g-systems--enabling-the-transformation-of-industry-and-society/white-paper--5g-systems--enabling-the-transformation-of-industry-and-society
73. Z Kotulski, T Nowak, M Sepczuk, M Tunia, R Artych, K Bocianiak, T Osko, J-P Wary, in *Proceedings of the 2017 Federated Conference on, Computer Science and Information Systems*, ed. by M Ganzha, L Maciaszek, and M Paprzycki. On end-to-end approach for slice isolation in 5G networks. Fundamental challenges, vol. vol. 11 (ACSIS, 2017), pp. 783–792. https://doi.org/10.15439/2017F228
74. IETF, multiprotocol label switching architecture (2001). https://tools.ietf.org/html/rfc3031. Accessed 12 Mar 2018
75. J Postel, Internet Protocol, STD 5, RFC 791. https://doi.org/10.17487/RFC0791. https://www.rfc-editor.org/info/rfc791. Accessed Sept 1981
76. IETF, Internet Protocol, Version 6 (IPv6) Specification (1998). https://www.ietf.org/rfc/rfc2460. Accessed 12 Mar 2018
77. A Manzalini, Buyukkoc C, P Chemouil, S Kuklinski, F Callegati, A Galis, M-P Odini, I Chih-Lin, J Huang, M Bursell, N Crespi, E Healy, S Sharrock, in *IEEE SDN White Paper*. Towards 5G Software-Defined Ecosystems. Technical Challenges, Business Sustainability and Policy Issues, (2016). http://servicearchitecture.wp.tem-tsp.eu/files/2016/07/White-Paper-IEEE-SDN-final_01-07-2016.docx
78. 3GPP TR 23.799 V14.0.0 Study on Architecture for Next Generation System (2016). http://www.3gpp.org/ftp//Specs/archive/23_series/23.799/
79. X An, C Zhou, R Trivisonno, R Guerzoni, A Kaloxylos, D Soldani, A Hecker, On end to end network slicing for 5G communication systems. Trans. Emerging Tel. Tech. **28**, e3058. https://doi.org/10.1002/ett.3058
80. X Li, M Samaka, HA Chan, D Bhamare, L Gupta, CH Guo, R Jain, Network slicing for 5G: challenges and opportunities. IEEE Internet Comput. **21**(5), 20–27 (2017). https://doi.org/10.1109/MIC.2017.3481355
81. X Foukas, G Patounas, A Elmokashfi, MK Marina, Network slicing in 5G: survey and challenges. IEEE Commun. Mag. **55**(5), 94–100 (2017). https://doi.org/10.1109/MCOM.2017.1600951
82. J Ordonez-Lucena, P Ameigeiras, D Lopez, JJ Ramos-Munoz, J Lorca, J Folgueira, Network slicing for 5G with SDN/NFV: concepts, architectures, and challenges. IEEE Commun. Mag. **55**(5) (2017). https://doi.org/10.1109/MCOM.2017.1600935
83. PK Chartsias, A Amiras, I Plevrakis, I Samaras, K Katsaros, D Kritharidis, E Trouva, I Angelopoulos, A Kourtis, MS Siddiqui, A Viñes, E Escalona, in *2017*

European Conference on Networks and Communications (EuCNC). SDN/NFV-based end to end network slicing for 5G multi-tenant networks, (2017), pp. 1–5. https://doi.org/10.1109/EuCNC.2017.7980670
84. S Gutz, A Story, C Schlesinger, N Foster, in *Proc.1st Workshop on Hot Topics in Software Defined Networks*. Splendid isolation: a slice abstraction for software-defined networks, (2012), pp. 79–84. https://doi.org/10.1145/2X00000.342441.2342458
85. R Kokku, R Mahindra, H Zhang, S Rangarajan, in *2013 Fifth International Conference on Communication Systems and Networks (COMSNETS)*. CellSlice: cellular wireless resource slicing for active RAN sharing (IEEE, 2013), pp. 1–10. https://doi.org/10.1109/COMSNETS.2013.6465548
86. P Rani, V Chauhan, S Kumar, D Sharma, A review on wireless propagation models. Int. J. Eng. Innov. Technol. (IJEIT). **3**(11), 256–261 (2014)
87. TK Sarkar, Z Ji, K Kim, A Medeuri, M Salazar-Palma, A survey of various propagation models for mobile communication. IEEE Antennas Propag. Mag. **45**(3), 51–82 (2003)
88. IEEE-SA Standards Board, Supplement to IEEE Standard for Information Technology - Telecommunications and Information Exchange Between Systems - Local and Metropolitan Area Networks - Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Higher-Speed Physical Layer Extension in the 2.4 GHz Band. September 1999. https://pdos.csail.mit.edu/archive/decouto/papers/802.11a.pdf
89. T Nowak, in *KSTiT 2017, Telecommunication Review-Telecommunication News*. Mathematical model of services isolation in network slicing (in Polish, 2017), pp. 8–9. https://doi.org/10.15199/59.2017.8-9.50
90. F Nife, Z Kotulski, in *Computer Networks. CN 2017., Communications in, Computer and Information Science (CCIS)*, ed. by P Gaj, A Kwiecien, and M Sawicki. Multi-level stateful firewall mechanism for software defined networks, vol. 718 (Springer, 2017), pp. 271–286. https://doi.org/10.1007/978-3-319-59767-6-22
91. Cognitive Network Management for 5G. The path towards the development and deployment of cognitive networking. 5G PPP Network Management and Quality of Service Working Group, Version: 1.02, 9-March-2017. https://www.researchgate.net/publication/315657928_Cognitive_Network_Management_for_5G
92. 5G Whitepaper: 5G Security Overview. Institute for Communication Systems, University of Surrey, August 2017. https://www.surrey.ac.uk/sites/default/files/5GIC-SSG-Security-Overview-WhitePaper-2017-08-02.pdf
93. Security Landscape, 5G PPP Security Working Group, June 2017. https://5g-ppp.eu/new-security-group-5g-ppp-white-paper-phase-1-security-landscape/
94. T Ciszkowski, W Mazurczyk, Z Kotulski, T Hossfeld, M Fiedler, D Collange, Towards quality of experience-based reputation models for future web service provisioning. Telecommun. Syst. **51**(4), 283–295 (2012). https://doi.org/10.1007/s11235-011-9435-2
95. J Konorski, P Pacyna, G Kolaczek, Z Kotulski, K Cabaj, P Szalachowski, in *Communications in Computer and Information Science (CCIS), vol.335, Recent Trends in Computer Networks and Distributed Systems Security, Part 1*. A virtualization-level future Internet defense-in-depth architecture (Springer-Verlag, Berlin Heidelberg, 2012), pp. 283–292. https://doi.org/10.1007/978-3-642-34135-9-29
96. R Artych, K Bocianiak, T Osko, in *Federated Conference on Computer Science and Information Systems*, ed. by M Ganzha, L Maciaszek, and M Paprzycki. Trustworthiness 5G Enabler, vol. 13, (2017), pp. 127–130. https://doi.org/10.15439/2017F235
97. Docker documentation. https://docs.docker.com/engine/docker-overview/#docker-objects. Accessed 12 Mar 2018
98. KVM project homepage. https://www.linux-kvm.org/. Accessed 12 Mar 2018
99. N Bhushan, J Li, D Malladi, R Gilmore, D Brenner, A Damnjanovic, RT Sukhavasi, C Patel, S Geirhofer, Network Densification: The dominant theme for wireless evolution into 5G. IEEE Commun. Mag (2014)