Proceedings of the Federated Conference on Computer Science and Information Systems pp. 783–792 DOI: 10.15439/2017F228 ISSN 2300-5963 ACSIS, Vol. 11

On end-to-end approach for slice isolation in 5G networks. Fundamental challenges

Zbigniew Kotulski
Tomasz Nowak
Mariusz Sepczuk
and Marcin Tunia
Warsaw University of Technology
Email: {z.kotulski; T.Nowak;
msepczuk; m.tunia}@tele.pw.edu.pl

Rafal Artych
Krzysztof Bocianiak
and Tomasz Osko
Orange Polska S.A.
Email: Rafal.Artych@orange.com
Krzysztof.Bocianiak@orange.com
Tomasz.Osko@orange.com

Jean-Philippe Wary
Orange Labs
France
Email: jeanphilippe.wary@orange.com

***Abstract*—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 goal of this paper is to present and examine the isolation capabilities and selected approaches for 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 proposed, which (if properly addressed) could be a step to E2E user's security based on slices isolation.**

I. Introduction

PROGRESS of work on the 5G network architecture can be characterized as the moment of movement from storming phase to forming phase. There is still a wide range of projects related to different areas of the 5G network [1] hence there are several main approaches to the architecture and implementation. Many 5G projects deal with network slicing aspects taking into consideration both technology and business perspectives. It is assumed that the ideas will continue to evolve for some time to give the final result in the foreseeable future.

Idea of isolation in the network is not new however currently considered technologies give new capabilities that can bring 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 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, an analysis of the isolation capabilities and selected approaches for its realization in network slicing context are presented. On 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 identifying 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 have to meet the expectations without breaching security standards. Business perspective has determined expected network parameters and introduced more open approach for 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 are real way to meet the needs but brings new challenges at the same time, introducing new potential vectors of attack. One of the hardest 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 we present known network slicing concepts, while Section 4 presents more 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. Finally, in section 7 conclusions and future research plans are presented.

II. Slicing: the 5G challenge

The new network concept (5G) will be more focused on business point of view than previous generations of mobile networks. Sets of requirements described in [2], [3], [4], [5] are very difficult or expensive to be satisfied in the whole network at the same time. 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 a services with some sets of specific properties (Key Performance Indicators, QoS/QoE parameters, etc.), which can be used to define new logical networks [6]. Each of these networks has its own 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 [2], [7], [8]. In the whole set of requirements with high probability exist many subsets of properties, which cannot be satisfied at the same time. However, reducing the set of requirements for a logical network could improve some selected properties critical for the service provided over this network.

A. The isolated slices

The logical networks described above are a 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) for service providers, other network operators and other allowed (authorized) users. The purpose for this feature is to make services and network more agile and adjustable to business and user's requirements or current network situation.

B. Security in a sliced network

This new concept with new elements brings new security questions and problems as these new elements also could bring new security issues. It is important to define who and how can use orchestrator and other modules to avoid security threats like exhaustion of resources or Denial of Service attack (DoS). 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 and solutions: slicing components can be implemented in firmware, OS kernel level, in the virtualization software systems or even in regular software. In this wide spectrum of environments, the slicing components may be provided by different vendors. Ensuring 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, i.e. by exploiting weak isolation providing system to reach resources in other slice with better parameters, lower costs or sensitive data stream. An attack on these properties could also be a part of more complex attack scenario (it could be subject to attack in the Attack Jungle concept [9]).

In slicing for 5G there are some common network services or functions like Mobility Management or AAA (Authentication, Authorization, Accounting) service [10], which are shared between more than one slice instance. This concept is in contrary with isolation property and should be considered how to solve this problem, especially in 5G, where we have more shared functions than in wired networks.

C. The major challenge in sliced 5G network

The key problem in 5G networks is implementation of the 5G RAN (Radio Access Network). The solution for some of problems could be using small cells in the mmWave [11]. Attenuation in this frequencies 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 [11]. This property naturally isolates traffic between different cells. Using two types of cells enables architecture, where part of data is transmitted by macro cells (i.e. data from C-Plane, what was described in [11]) and rest of them is transmitted by small cells (i.e. data from U-Plane). In slicing terms one can look at this as a special meta-slice, which allows User Equipments (UE) to communicate with RAN and CN (Core Network).

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 [11] and it recognizes messages depending on the signal power level. In this case the Base Stations (BS) 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 [11].

III. Concepts of network slicing

A. Network Slicing definition

Network slicing is one of the crucial technologies that enables flexibility, 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 was introduced in the paper [12], 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 [13]:

- 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 3rd parties, so the Service Instance can be created by both operator services and 3rd parties services.

A Network Slice Instance is a set of (virtualized) network functions implemented at resources which enable running these network functions. It forms a complete instantiated logical networks to 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 isolation. To create a Network Slice Instance, a network operator uses a Network Slice Blueprint (description of the structure, configuration and the flows and how 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 instance of network slices.

The Resources Layer contains both physical and logical resources. The Network Slice Instance can consist of Subnetwork 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.

B. *Vertical and horizontal slicing*

Another slicing concept is described in [14], where the authors describe two approaches to network slicing: vertical and horizontal. On the vertical network slicing one network is sliced into multiple network slices, each designed and optimized for particular services or applications. The horizontal network slicing enables sharing of resources between nodes and network devices. Both approaches can be implemented in parallel and they can work together.

C. *E2E Network Slicing*

The concept of Network Slicing in 5G refers to three areas [15], [16]: at the air interface, in the RAN and in the CN.

1) Network slicing at the air interface: The idea of Network Slicing of Air Interface refers to proper partitioning of physical radio resources (PHY layer), mapping them into logical resources and creating the operations of MAC (Media Access Control) and higher layers based on the logical PHY resources.

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. Besides two aspects should be investigated:

- The Radio Access Type (RAT) which supports services provided by a particular slice,
- The proper configuration of RAN capabilities with interfaces. It applies also to a correct cell deployment in every slice based on requirements. Based on factors such as QoS requirements, traffic load or type of traffic, the RAN architecture should be properly tailored to each slices.

This is a huge challenge because 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).

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 in order to bring flexibility in management. Supporting the SDN-like separation of planes is one of the main principles of 5G core network architecture, because it allows, see [17]:

- 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.

IV. NETWORK SLICING: ISOLATION, MANAGEMENT, SECURITY

A. *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 requirements and usage scenarios for slicing. 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 different ways and constitute a set of properties chosen according to implementation needs. After analysis of 5G network slicing security issues [18] 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 slice,
- Reliability assurance of different pieces of physical equipment which 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 (NF) and virtualized NFs,
- Isolation of slices with one user equipment connected to multiple slices at a time.

Not all of the properties should be implemented in each solution. There can be subsets of those properties chosen in order to meet specific requirements. Isolation may be achieved by different means, including [19]:

- 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 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 (Multi-Protocol 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 [20].

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 [21].

B. 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 [22] defines several areas of potential vulnerabilities including firmware abuse, eavesdropping, man-in-the-middle, APIs abuse, resource exhaustion, packet flooding and more. Research [23] 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 [24], [25]. 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 under 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.

C. Isolation in wireless domain

In wireless domain there are some techniques for slices isolation which are dedicated especially for this domain. This is because of special properties of air interfaces and medium. According to [8] 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 (WiFi) 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 [8]:

- Virtual Basestation [26] in WiMAX implements slices' isolation with traffic shaping techniques in downlink,
- CellSlice [27] in WiMAX implements slices' isolation with slice scheduling and traffic shaping in uplink and sustained rate control in downlink,
- The papers [28], [29] describe assigning resources in LTE with PRB scheduling in downlink,

- Virtual WiFi [30] describes client virtualization in 802.11 networks using slice scheduling.

D. 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, makes accounting for transmission and cleans after-effects 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. [31], [32], [33]. The papers presenting 5G management and orchestration, which is this part of management that can be automated, usually consider the ETSI NFV-MANO [34] as a reference model. 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 [35]) 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., [36], [37]. The systems are compatible because they have plane-based/layered structure and both of them 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., [6], [38], [39], [40]). Such an approach enables application of the ETSI NFV-MANO system directly for a single domain or instance and provide a supervision over a number of 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.,[41], [42], [43].

Another aspect of MANO in a multi-domain networks was considered in paper [44]. 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 in frames 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., [45]), where decision rules are negotiated among network elements according to their own particular interests.

Enhancing slicing property of the expected 5G networks led to extended ETSI NFV-MANO systems. Some approaches try to make an order in information flow in MANO (which is a critical and still unsolved problem) introducing it as a specific ETSI NFV-MANO service, see [46]. The other paper adds new orchestration functions dedicated specially for slicing, slicing in multi-tenant and multi-domain environments (see [47]).

All MANO 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 a performance isolation, which is natural in 5G slices concept. For a stronger, secure (cryptographic) isolation, a new orchestration aspect should be taken into account, 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 MANO scheme must be proposed, where isolation establishment at each stage of a slice lifetime is considered. The scheme must take into account also such elements as: slice chaining, isolation establishment, and isolation checking and monitoring.

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 heavy to be implemented and controlled. Thus, should be considered a single management and orchestration system or it is 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 a few information flows between MANO subsystems to specify.

V. Concerned issues in 5G networks

5G, as a future generation of telecommunications standards, faces new issues every day when already posed or identified tasks are solved. In this section a number of 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 [48] presenting actual issues inspired by conditions resulting from techno-economic conditions and policy constraints and proposing a change of paradigms in the design and operation of future telecommunications infrastructures dedicated to 5G networks. The main issues identified in the paper [48] 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 end-to-end 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, as a consequence, network reliability and security.

The recent technical report [49] 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 regards 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?
- The procedure(s) for selection of a particular Network Slice for a UE;
- How to support Network Slicing Roaming scenarios ?
- How to enable operators to use the network slicing concept to efficiently support multiple 3rd parties (e.g. enterprises, service providers, content providers, etc.) that require similar network characteristics ?

Future networks expectations undergo different trends, visions and requirements which must be taken into account to obtain effective, flexible and reliable systems. Among them, the crucial are: 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 particular, end-to-end slicing approach. Paper [50] addresses the key issues of how 5G devices may be enabled to discover, select and access the most appropriate E2E network slices. Except of 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.

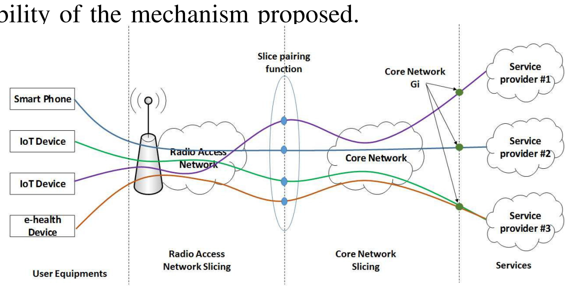

Fig. 1. The slice chaining concept, based on [51]

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 [10]. The service chaining is a technique for selecting and steering data flows using different kind 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.1) is defined as a way to establish one E2E connection through RAN and CN networks to a particular 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 slices and their independence. Thus, the isolation of resources/slices should be provided. In the following Section 6 we present a number of 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.

VI. Towards 5G isolated slicing: new challenges

As a result of the investigations and analyses the following key challenges are proposed. Considering them should result in providing an effective sliced network with E2E secure isolation.

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

According 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. In order to assure the proper quality of design for network slices isolation there should be developed a framework covering requirements gathering and analysis. Such normalized approach would help network operators to take into account 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 exposing 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 [52]:

- Isolation of a traffic: All slices using the same network resources, so the network slices should ensure that data flow of one slice does not move to another
- Isolation of a 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/network capacity.
- Isolation of a 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.
- Isolation of a storage: Data related to a particular 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 were done in the SDN idea but still they are far from being mature. In context of 5G network slicing it 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 other, 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. On the basis of this risk analysis there should be proposed countermeasures to minimize the risk. Technology can be connected 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).

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.

B. 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.[50],
- 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. A 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 particular 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 we 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.

C. 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 be connected with 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 to solve the readers-writers problem between slices in reference 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.

D. Providing a method of creation 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 degenerates 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 problems. In the fibers, we have the FWM (Four-Wave Mixing) problem: two different wavelengths produce unwanted new two wavelengths, which degenerates output signal from fiber. This effect can be minimized by properly chosen wavelength, but it limits the number of dynamically created isolated slices (and there are 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 with the CN and this part should be optimized in order 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 part of 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 end-to-end 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: 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 properly creation slices inside each slice domain (RAN, CN and other) and in next step try to look after E2E slices' isolation. The slices in each domain can be created independently, but simultaneously creation could create 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 (maybe for a limited period of time).

E. 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 of 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 (Service Level Agreement).

Accounting is connected with 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.

F. 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, e.g., for isolated slices establishment and for their usage. It must also cover security management, 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 users assignment 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 a context of network management is fulfillment of legal conditions related to telecommunication networks and network security. Such conditions can be different for different 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 be 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 some access control delivered at slice level with end to end isolation (ciphering) in a way appropriate for all domains.

G. Unified interface (API) and protocol for access 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 common way. There should exists a negotiation protocol between orchestrators from different Network Operators which uses some slicing maintenance policy. The protocol should satisfy 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, 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 accepted this earlier. 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.

VII. Conclusions and Next Steps

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, in order 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) concrete 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. In order to define an abstraction for different resources it is necessary to specify attributes allowing unambiguous definition and rigorous verification of isolation level in a given 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 long discussions held between research groups of Orange Labs and Warsaw University of Technology last year. Proposed tasks, although they cover a wide range of issues related to isolated network slicing, do not cover all important areas for slice isolation. We deliberately skipped the areas related to communication hardware-based technologies, concentrating on those solutions which are management-related and which are expected to be software-based.

The next steps of the research are: 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.

References

[1] *CORDIS web page*, http://cordis.europa.eu/

[2] *Dynamic end-to-end network slicing for 5G*, Nokia White Paper, 2016.

[3] Shimojo, T. et.al., "Future mobile core network for efficient service operation", *Proc. 1st IEEE Conf. on Network Softwarization (NetSoft)*, pp.1-6, 2015, doi: 10.1109/NETSOFT.2015.7116190.

[4] Herzog, U. et.al., "Quality of service provision and capacity expansion through extended-DSA for 5G", *Trans. Emerging Telecommunications Technologies*, 27(9), pp.1250-1261, 2016, doi: 10.1109/EuCNC.2016.7561032.

[5] Nakao, A. et.al., "End-to-end Network Slicing for 5G Mobile Networks", *J. Inf. Processing*, vol.25, pp.153-163, 2017, doi: 10.2197/ipsjjip.25.153.

[6] *View on 5G Architecture*, 5G PPP Arch. Working Group, 2016.

[7] Bulakci, O., "Towards sustainable 5G Networks. Vision & Design Principles for New Horizons", *IEEE Vehicular Technology Conf.*, Boston 2015.

[8] Richart, M. et.al., "Resource Slicing in Virtual Wireless Networks: A Survey", *IEEE Trans. Network and Service Management*, 13(3), pp. 462-476, 2016, doi: 10.1109/TNSM.2016.2597295.

[9] Abdulla, P.A., Cedergerg, J., Kaati, L., "Analyzing the Security in the GSM Radio Network Using Attack Jungles", *Proc. 4th Int. Symp. Leveraging Applications, ISoLA 2010*, pp.60-74, Greece 2010, doi: 10.1007/978-3-642-16558-0_8.

[10] Yoo, T., "Network Slicing Architecture for 5G Network", *7th Int. Conf. Information and Communication Technology Convergence*, pp.1010-1014, IEEE, Korea 2016, doi: 10.1109/ICTC.2016.7763354.

[11] Ma, Z. et.al., "Key techniques for 5G wireless communications: network architecture, physical layer, and MAC layer perspectives", *Science China Information Sciences*, 58(4), 2015, doi: 10.1007/s11432-015-5293-y.

[12] Peterson, L. et.al., "A blueprint for introducing disruptive technology into the Internet", *ACM SIGCOMM Computer Communication Review*, 33(1), pp.59-64, 2003, doi: 10.1145/774763.774772.

[13] Chapman, C., Ward, S., *Description of Network Slicing Concept*, NGMN Alliance 2016.

[14] Li, Q. et.al., "End-to-end Network Slicing in 5G Wireless Communication Systems", *Proc. ETSI Workshop on Future Radio Technologies and Air Interfaces*, pp.1-4, 2016.

[15] Li, Q. et.al., "An end-to-end network slicing framework for 5G wireless communication systems", *arXiv:1608.00572 [cs.NI]*, 2016.

[16] *5G Americas White Paper: Network Slicing for 5G and Beyond*, 2016.

[17] *A vision of the 5G core*, Ericsson 2016.

[18] Harel, R., Babbage, S., *5G security recommendations Package 2: Network Slicing*, NGMN Alliance 2016.

[19] Viswanathan, A., Neuman, B.C., "A survey of isolation techniques", *Univ. Southern California, Inf. Sc. Ins.*, 2009.

[20] *Applying SDN Architecture to 5G Slicing*, Open Networking Foundation 2016.

[21] Del Piccolo, V. et.al., "A Survey of Network Isolation Solutions for Multi-Tenant Data Centers", *IEEE Comm. Surveys and Tutorials*, 18(4), pp.2787-2821, 2016, doi: 10.1109/COMST.2016.2556979

[22] *SDN security project*, http://sdnsecurity.org/index.html.

[23] Yoon, Ch., Lee, S., "Attacking SDN Infrastructure: Are We Ready for the Next-Gen Networking?" *BlackHat* 2016.

[24] *DELTA: A Penetration Testing Framework for Software-Defined Networks*, Open Networking Foundation 2016.

[25] Lee, S. et.al, "Athena: The Network Anomaly Detection Framework for SDN", *IEEE/IFIP Int. Conf. Dependable Systems andNetworks*, 2017, doi: 10.1109/DSN.2017.42

[26] Bhanage, G. et.al., "Virtual basestation: architecture for an open shared WiMax framework", *Proc. 2nd ACM SIGCOMM Workshop on Virtualized Infrastructure Systems and Architectures*, pp.1-8, ACM 2010, doi: 10.1145/1851399.1851401

[27] Kokku, R. et.al., "Cellslice: Cellular wireless resource slicing for active RAN sharing", *5th Int. Conf. Communication Systems and Networks (COMSNETS)*, pp.1-10, IEEE 2013, doi: 10.1109/COMSNETS.2013.6465548

[28] Zaki, Y. et.al., "LTE wireless virtualization and spectrum management", *3rd Joint IFIP Wireless and Mobile Networking Conf. (WMNC)*, pp.1-6, IEEE 2010, doi: 10.1109/WMNC.2010.5678740

[29] Zaki, Y. et.al., "LTE mobile network virtualization", *Mobile Networks and Applications*, 16(4), pp.424-432, 2011, doi: 10.1007/s11036-011-0321-7

[30] Xia, L. et.al., "Virtual wifi: bring virtualization from wired to wireless", *ACM SIGPLAN Notices*, 46(7), pp.181-192, 2011, doi: 10.1145/1952682.1952706

[31] *Network Functions Virtualisation (NFV). Network Operator Perspectives on Industry Progress*, ETSI NFV Whitepaper 3, 2014.

[32] Son, H.J., Yoo, Ch., "E2E Network Slicing Key 5G technology : What is it? Why do we need it? How do we implement it?", *Netmanias web page*, 2015.

[33] *The 5G Infrastructure Public Private Partnership web page*, https://5g-ppp.eu/.

[34] ETSI GS NFV-IFA 009 V1.1.1 (2016-07) *Network Functions Virtualisation (NFV); Management and Orchestration; Report on Architectural Options*.

[35] *ETSI NFV standards web page* http://www.etsi.org/technologies-clusters/technologies/nfv/.

[36] Nejabati, R. et.al., "SDN and NFV Convergence a Technology Enabler for Abstracting and Virtualising Hardware and Control of Optical Networks", *Optical Fiber Comm. Conf. and Exhib. (OFC)*, 2015, doi: 10.1364/ofc.2015.w4j.6.

[37] Munoz, R. et.al., "Integrated SDN/NFV Management and Orchestration Architecture for Dynamic Deployment of Virtual SDN Control Instances for Virtual Tenant Networks", *J. Optical Comm. and Networking*, 7(11), pp.B62-B70, 2015, doi: 10.1364/jocn.7.000b62.

[38] Contreras, L.M. et.al., "Orchestration of Crosshaul Slices From Federated Administrative Domains", *Eur. Conf. Networks and Comm. (EuCNC)*, pp.220-224, Athens 2016, doi: 10.1109/eucnc.2016.7561036.

[39] Zhou, X. et.al., "Network Slicing as a Service: Enabling Enterprises' Own Software-Defined Cellular Networks", *IEEE Comm. Mag.*, 54(7), pp.146-153, 2016, doi: 10.1109/mcom.2016.7509393.

[40] Rost, P. et.al., "Mobile Network Architecture Evolution toward 5G", *IEEE Comm. Mag.*, 54(5), pp.84-91, 2016, doi: 10.1109/mcom.2016.7470940.

[41] Moens, H., De Turck, F., "Customizable Function Chains: Managing Service Chain Variability in Hybrid NFV Networks", *IEEE Trans. Network and Service Management*, 13(4), pp.711-724, 2016, doi: 10.1109/tnsm.2016.2580668.

[42] Halpern, J., Pignataro, C., "Service Function Chaining (SFC) Architecture", *RFC 7665*, IETF 2015, doi: 10.17487/rfc7665.

[43] Bari, Md.F. et.al., "Orchestrating Virtualized Network Functions", *IEEE Trans. Network and Service Management*, 13(4), pp.725-739, 2016, doi: 10.1109/tnsm.2016.2569020.

[44] Stanik, A., Koerner, M., Kao, O., "Service-level agreement aggregation for quality of service-aware federated cloud networking", *IET Networks*, 4(5), pp.264-269, 2015, doi: 10.1049/iet-net.2014.0104.

[45] Cherrier, S. et.al., "Fault-recovery and Coherence in Internet of Things Choreographies", *IEEE World Forum on Internet of Things (WF-IoT)*, pp.532-537, Seoul 2014, doi: 10.1109/wf-iot.2014.6803224.

[46] Mamatas, L., Clayman, S., Galis, A., "Information Exchange Management as a Service for Network Function Virtualization Environments", *IEEE Trans. Network and Service Management*, 13(3), pp.564-577, 2016, doi: 10.1109/TNSM.2016.2587664.

[47] "Functional Network Architecture and Security Requirements", *5G-NORMA Deliverable D3.1*.

[48] Manzalini, A. et.al., "Towards 5G Software-Defined Ecosystems. Technical Challenges, Business Sustainability and Policy Issues," *IEEE SDN White Paper*.

[49] 3GPP TR 23.799 V14.0.0 *Study on Architecture for Next Generation System*, 2016.

[50] An, X. et.al., "On end to end network slicing for 5G communication systems", *Trans. Emerging Tel. Tech.*, 28:e3058, doi: 10.1002/ett.3058.

[51] *5G systems - Enabling industry and society transformation*, Ericsson White Paper, UEN 284 23-3244, 2015.

[52] Gutz, S. et.al., "Splendid Isolation: A Slice Abstraction for Software-Defined Networks", *Proc. 1st Workshop on Hot Topics in Software Defined Networks*, pp.79-84, 2012, doi: 10.1145/2342441.2342458.