Security and Resilience in 5G: Current Challenges and Future Directions

Ghada Arfaoui, José Manuel Sanchez Vilchez, Jean-Philippe Wary
Orange Labs
Châtillon, France
Email: {ghada.arfaoui; jose2.sanchez; jeanphilippe.wary}@orange.com

***Abstract*—5G tends to be a multi-layered, multi-actor, and multi-access mobile network in order to fulfill the stringent availability, security, privacy and resilience requirements that are usually contradictory. In this paper, we propose a 5G vision based on softwarization. We provide a non-exhaustive list of current security, trust and resilience issues that are critical to be explored in 5G. We finally give some directions to overcome these issues.**

I. Introduction

The increasing computation and memory capabilities of mobile devices, namely smartphones, drive them to replace the use of laptops and to become a life style [1]. Smartphones are more and more used for daily activities like shopping, booking, transport, banking, among others. All these new usages are creating huge and massive connectivity needs. To satisfy the dramatically growing need of users and things in terms of connectivity and network availability, the mobile networks will be in the core of the evolution and innovation. According to Porter [2], the main triggers of innovation and competition in industry are (i) threat of new entrants, (ii) threat of substitute product, and (iii) consumer power. Currently, in mobile networks, these factors are present. This leads to the next mobile generation, so called "5G".

5G is claimed to satisfy the dramatically growing need of users and things for the imminent 2020 horizon. Indeed, 5G networks are expected to be a multi-access network in order to deserve about 7 trillions of heterogeneous connected things, amongst which 20 billions are human-oriented devices, as stated by the 5G-PPP partnership [3]. These performance must be achieved whilst having a similar cost and energy consumption as the current networks. In METIS project [4], [5], one of the leading projects in this area, these objectives have been formalized as follows. Compared to previous mobile network generations, 5G should provide:

- Up to 1000 times higher mobile data volume per area,
- Up to 100 times higher number of connected devices,
- Up to 100 times higher user data rate,
- Up to 10 times longer battery life for Massive Machine Communication type devices, and
- Up to 5 times reduced end-to-end latency.

The one-network-fits-all concept must answer these demanding and ambitious objectives. This is why the transition towards 5G is much more abrupt, meaningful and challenging compared to any of the previous transitions. To do so, 5G should be empowered with three main principles:

- *Programmability:* network programmability is mainly about Network Softwarization. It enables elastic and highly flexible networks to rapidly deploy new and various services, in a customized way, and with reduced consumption. Although its definition and architecture are still at its infancy stage, it trends to rely on Software-Defined Networking (SDN) and Networks Function Virtualization (NFV).
- *Automation:* it is the next obvious step after the setup of the programmability in 5G networks. This should shorten the service life-cycle from months to minutes and even seconds. It also introduces DevOps principles which tend to join together both design and operation stages to reach a fast and agile network operation.
- *Intelligence:* to cope with the overwhelming amount of data coming from trillions of devices and best meet the objectives of 5G, 5G networks need to consider new management approaches more accurate and practical. One way is to enable and use machine-learning based algorithms in the network management.

This evidences that some management aspects in 5G may have to be conceived from scratch. Additionally, to fully enjoy the principles previously cited, 5G networks should be designed in such a way that security and resilience are taken into account as a cornerstone feature in both design and operation stages. In 5G, "build first and secure later" typical paradigm should be replaced by "security and resiliency by design" and "security and resiliency by operation".

The purpose of this paper is to give an insight on security, trust and resilience challenges brought by 5G and propose potential solutions. The paper is organized as follows. In Section II, we give definitions of virtualization technologies that could be used in the design of 5G networks. Section III describes our 5G network vision. Later, we explain other SDN-NFV based 5G design. We detail the new trust challenges and give likely mechanisms to overcome it in Section V. Then, in Section VI, we present the major security and resilience challenges and our proposals to overwhelm it. In Section VII, we focus on challenges related to privacy aspect and regulations. Section VIII gives an overview about work done about 5G security, trust and resilience network in European projects,

standards and literature. We conclude in Section IX.

II. Background

5G is expected to provide a more flexible and dynamic network. To the best knowledge of the authors, at the writing of the paper, there is not a standardized vision of the 5G functional architecture. It is still a matter of active discussion among the most important worldwide standardization organizations and between telecom operators and vendors. However, there is some consensus on the choice of virtualization technologies, such as Network Function Virtualization (NFV), Software-Defined Networking (SDN), and new concepts like network slicing, to implement 5G networks. In the following, we give some definitions of these virtualization technologies.

a) Software-Defined Networking (SDN): is a novel network architecture based on abstraction, open interfaces, and control-data planes separation. Open Networking Foundation (ONF) defines SDN as "the physical separation of the network control plane from the forwarding plane, where the control plane controls several devices" [6]. SDN architecture, depicted in Figure 1, is composed of data, control, application and management planes. Data plane is composed of SDN resources transporting the traffic belonging to the infrastructure layer, i.e., OpenFlow switches, and the hosts/servers acting as traffic sources and sinks. Control plane mediates between data and application planes. It is based on a given control software intelligence which is embedded in the so called SDN controllers, which dictate the forwarding rules to the data plane. Application plane is composed of SDN applications that program the network through exposed Application Programming Interfaces (APIs). Management plane is transversal to the rest. The main advantages of SDN are the programmability of the data plane by means of SDN applications independently from the underlying physical architecture.

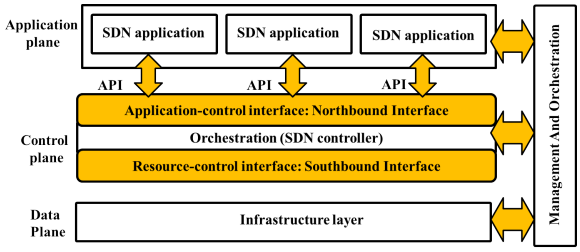

Fig. 1. SDN layered architecture [7]

b) Network Function Virtualization (NFV): is a networking initiative led by Telcos [8], to embed current network functions, (e.g., ciphering, firewall, load balancing, TCP accelerators, concentrators, DNS, QoE Management, video optimizers) in commodity hardware (e.g., high-volume standard servers, storage and switches). Network functions become then Virtualized Network Functions (VNFs). The NFV reference architecture, as shown in Figure 2, defined by ETSI [9] introduces a transversal block called Management and Orchestration (MANO). This entity is composed of the NFV Orchestrator(NFVO), the VNF Manager (VNFM), and the Virtualized Infrastructure Manager (VIM). NFVO manages the life-cycle of the instantiated networking services. VNFM manages the life-cycle of its instantiated VNFs. VIM allocates the virtual resources required by the NFVO and/or the VNFM on the physical infrastructure.

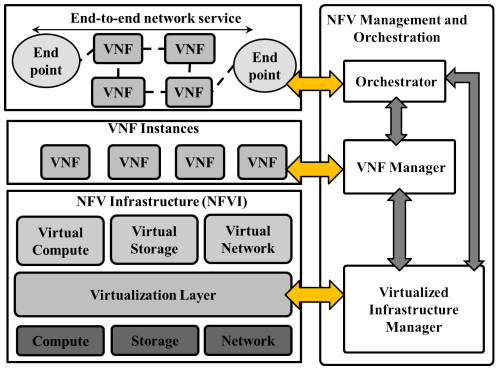

Fig. 2. NFV high level architecture [8]

The main advantages of the NFV approach are to reduce power consumption, maintenance and integration costs and time-to-market. NFV also allows to remove the vendor lock-in barrier. In addition, it enables networking services to be flexibly instantiated and scaled, according to network traffic demands, at run-time by making an elastic usage of the compute, storage and networking resources.

c) A network slice: is a logical dedicated network composed of virtualized and non-virtualized resources that can be instantiated and customized to fulfill a set of requirements [10].

III. Our 5G vision: an SDN-NFV based approach

After recalling each of these softwarization paradigms, we give some insights on how it can implement a 5G network. The core idea is to realize 5G network slicing with SDN/NFV. Thus, a Mobile Network Operator (MNO) builds a 5G network using hardware infrastructures from one or several "Infrastructure providers" and Virtualized Network Functions (VNFs) designed by one or various "VNF providers", then, sets up slices for service providers and verticals. The SDN-NFV based slicing for 5G would enable to tailor the network to the particularities and requirements of different use cases and services. For instance, we can define a slice for an e-health service or a remote surgery service with high resilience, security, privacy and availability requirements, then, a slice for ordinary broadcasting services.

We consider, in our approach, that every service or use case is delivered over a slice composed of a VNF chain connected through virtual links established by an SDN controller. We conceive a 5G network as a three-layered slicing architecture, as drawn in Figure 3. The architecture is composed of the application layer, the virtualized infrastructure layer, and the physical infrastructure layer. The application layer is where the end-user applications are defined and translated into network services with their corresponding descriptors and virtual

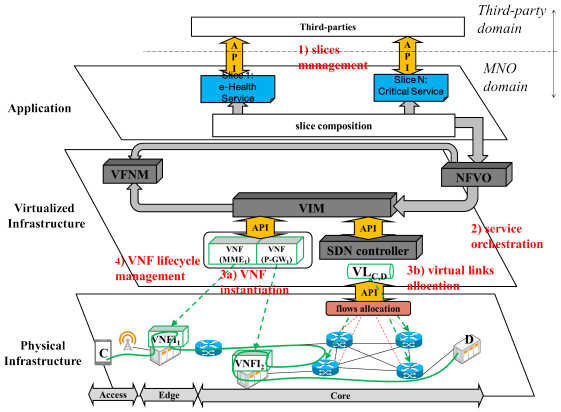

Fig. 3. 5G slicing architecture with SDN/NFV

resources. The virtualized infrastructure layer is where the virtual resources are instantiated, mapped and monitored. The physical infrastructure layer is composed of the access edge and core segments. The edge and core segments could then be composed of dumb OpenFlow switches managed by the SDN controller.

The work-flow to deploy slices in 5G encompasses four phases, tagged in red color in Figure 3:

1) *Slice Management:* The first phase consists of the definition and management of slices associated to use cases and services. This phase is operated by third-parties at the application plane through Application Programming Interfaces (APIs) or slicing portals.
2) *Service Orchestration:* The second phase consists of the orchestration of the underlying network services to the defined slices. NFVO ensures this phase at the virtualized infrastructure level.
3) *VNF allocation:* This phase is run in the virtualized and physical infrastructure layers. It consists of preparing a network service slice. This latter is depicted by a VNF Forwarding Graph (VNF FG) containing all the virtual resources to be allocated. First, the VIM instantiates the VNFs (3a). Second, the SDN controller allocates the virtual links to connect those VNFs (3b).
4) *VNF Life Cycle Management:* This phase involves triggering the appropriate scaling operations in case of any degradation or failure at VNF level.

The key advantage of implementing 5G slicing with SDN/NFV is the flexibility and rapid slices deployment according to the services requirements namely performance and security requirements. Indeed, an SDN-NFV based slicing approach would provide the following features:

- The separation of the control plane from the user/data plane through SDN. This enables the *programmability* principle that we cited previously in section I.
- The removal of the intelligence from the network nodes and its integration in control, application, and management layers. This feature facilitates the *automation* principle defined in section I.
- The elasticity to run and manage the life-cycle of virtualized network services, at run-time, through the NFV framework, and
- The ability to customize slices, i.e., omit / adapt / allocate / migrate specific network functions for a given service (for instance, we may not need mobility management functions for fixed services). The last two features enable the *intelligence* principle mentioned in section I .

Altough SDN and NFV are thought to be "better together" by the IT and telecommunication industry in order to exploit their potential benefits, this marriage implies new challenges namely implementation, trust, security and resilience challenges. We detail these new challenges in the following sections.

IV. SDN/NFV BASED 5G IMPLEMENTATION CHALLENGES

The implementation of combined SDN/NFV infrastructure for 5G networks is quite a controversial challenge as there are several ways of implementation. Evidenced by the lack of consensus on the position of some SDN elements within the NFV framework, the way to combine SDN and NFV is still under discussion. Indeed, the SDN controller and the SDN applications can be placed in multiple parts of the NFV reference framework.

An SDN controller can be implemented:

1) *As part of the VIM.* This is the most natural position where the VIM (e.g. Openstack) allocates computation resources, then, contacts the SDN controller through its northbound interface to allocate network resources.
2) *As a VNF or a Physical Network Function (PNF).* This position implies that its life-cycle is managed by the VNFM. In such a position, this VNF performs only control plane functions
3) *As part of the NFV Infrastructure (NFVI)* (i.e., the bottommost block in Figure 2). In this location, it would be acting as a network hypervisor providing virtualized networks on top of the physical resources.
4) *As part of the Operations Support System/Business Support System (OSS/BSS).* OSS/BSS is where the services are defined, and is directly connected to the NFVO in the NFV reference architecture. At this position, the SDN controller would not react at millisecond scale being therefore dedicated to rather static and high-level tasks.

SDN applications can be also located in several locations:

1) *As a VNF/PNF.* If the SDN applications are implemented as a VNF, the SDN controller could be also implemented as a VNF/PNF to reduce the latency to communicate both entities.
2) *As part of the VIM.* If the SDN applications are implemented inside the VIM, the SDN controller could also be integrated within the VIM to reduce the latency.
3) *As part of an Element Manager (EM).* As the EM embeds the SDN applications, it is worth to implement the SDN controller as a VNF. This is to manage it from the SDN application which is now part of the EM and hence reduce the latency.

4) *As part of the OSS/BSS.* If the SDN applications are embedded at OSS/BSS level is rather preferable to locate the SDN controller at this level and not at an infrastructure level to reduce the latency

In addition to this lack of consensus on the implementation, the ETSI NFV draft in [11] introduces two types of SDN controllers: the infrastructure SDN controller and the tenant SDN controller. The infrastructure SDN controller is managed by the VIM. It is in charge of establishing virtual links among the VNFs. The tenant SDN controller would be located in the EM layer (located just below the OSS/BSS layer). Contrarily to the SDN infrastructure controller which reacts at *ms* scale, the tenant SDN controller will require higher reaction time because it has a much higher position than the infrastructure SDN controller. Consequently, we can have a hierarchical approach where the tenant SDN controller would act as hierarchically superior entity and needs to be coordinated with the infrastructure SDN controller.

V. Trust and Liability Management

Because of the new technologies and concepts described previously, the three-party trust model (i.e. end user, MNO and service provider) considered in the current mobile generations will be replaced by models that include new semi-trusted parties. 5G will be a multi-actor mobile network where several parties cooperate in the delivery of a given service.

Consider for instance, a VNF ensuring the Mobility Management function (MME VNF). This VNF involves the following actors and roles: VNF provider, the slice owner, the slice provider, the VNF manager, and the infrastructure provider, all shown in Figure 4. This VNF is provided by a VNF Provider "A", runs within a slice that belongs to a Slice Owner "B" and in turn is managed by a Slice Provider "C". However, this VNF is managed by a VNF Manager "D" and runs over a given hardware belonging to a given Infrastructure Provider "E". All those roles can be assured by the MNO. In this case, we end up in the same situation as current mobile network generations where the MNO is the "owner" of the mobile network and also main responsible for any issue (financially responsible). However, if the roles are allocated to different entities/actors, the main-owner-responsible system model applied in the current mobile networks is not any more relevant. For instance, if the VNF had a security or functional issue (e.g., unavailability, under-performance, security/isolation breaches, or non-compliance with security policies), the responsibility would need to set to any of the aforementioned actors (A,B,C,D,E).

In such a complex environment, trust among parties becomes critical. Trust is the first stone towards tracing and scoring the effort and performance of the different actors involved in a given service to manage its SLA. This trust and liability system can be built on various mechanisms. Indeed, reputation propagation mechanisms (based on metrics such as the security and resiliency mechanisms used by each actor) allow to pinpoint the actor responsible of service outages. The trust and liability system can also be based on remote

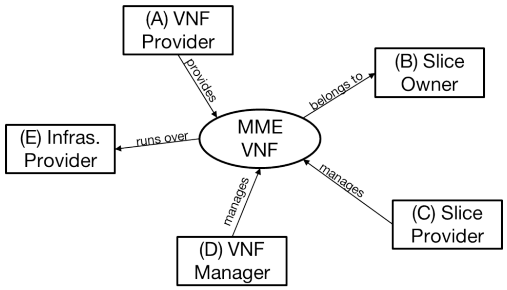

Fig. 4. An example of the MME VNF's dependencies

or local attestation of a given property like the code integrity, the trustworthiness of the execution environment, the isolation of a slice and so forth. The capabilities of Trusted Execution Environment in network nodes could also re-enforce the security of this system. Besides, VNF Certifications can be a tool to build liability chains. For instance, as defined in ETSI NFV in [12], VNF certification mechanisms can certify the integrity of the VNF before being uploaded into the VNF catalog. This will enable the MNO to decide to deploy the VNF based on its trustworthiness (appropriate behavior/ not misuse of NFVI resources) and the suitability (compliance, performance, etc.). Naturally, in addition to the technical solutions, agreements between different actors are needed.

This multi-actor environment raises two main challenges. The first challenge for the MNO is to be able to verify the state of the mobile network and ensure is stability. Overcoming this challenge is a step in the security and resilience management of 5G (cf. Section VI). The second challenge for the MNO is to ensure the security and privacy of end user data while adhering to Lawful Interception (LI) requirements and proposing enhanced services (cf. Section VII).

VI. Security and Resilience management

The principle security objective of 5G networks is to provide a higher security level compared to current mobile networks. Hence, 5G networks are expected to at least provide solutions to security issues identified in current mobile networks. Additionally, 5G should manage the security issues related to softwarized networks.

A. Network Access

A major key of Radio Access Network security is the strong authentication of end users / things regardless the device capabilities and the targeted service. In a simplified manner, the security of an authentication process is based on two elements: the applied cryptographic algorithm and the credential storage. Consequently, a restricted resource device or an old device should not be able to apply weak cryptographic algorithms to ensure the authentication (this was possible in previous mobile networks). This kind of devices can rely on secure computation delegation mechanisms to reach the required security level during the authentication. In addition, even if the targeted service applies an authentication

process, the network authentication must still be mandatory. As regards end user / thing credentials, it must be stored in a tamper resistant and highly secure environment that has been carefully certified. Indeed, a compromised credential can lead to the compromise of all the user / thing associated services.

B. Network Platform

As a dynamic network, 5G will experiment the addition and deletion of network elements / nodes (physical or virtualized) in an automated way and without any human interaction. The automated manner introduces new security and resilience challenges namely the risk of accepting a malicious node. We can distinguish two types of malicious nodes: active or passive nodes. An active malicious network node may perform a set of attacks (for instance in critical mobile network nodes such as Home Subscriber Server, HSS) and provoke a degradation of the network QoS or even a disruption. A passive malicious node can merely enable information leakage without any tangible impact on the network. Information leakage is not only a privacy breach, it can also be a pre-step of a more widespread attack (e.g., DDoS). In these circumstances, network nodes authentication should be a must in 5G networks. Before any node addition, the node must prove that it is authorized to get attached to the network and has not been compromised. This requirements can be accomplished based on secure attestation protocols consolidated by Trusted Execution Environments.

C. SDN-NFV based networks

Softwarized networks heavily rely on a logically centralized control, which takes the forwarding decisions at the control plane and sends them to the data plane with a certain level of abstraction. This approach simplifies the forwarding devices to just execute the forwarding decisions. However, three main risks come as consequence from the centralization: (i) attacks towards the control plane, (ii) lack of scalability and possible congestions and bottlenecks in the control plane to handle all the requests coming from the data plane, and the (iii) lack of resilience of the control plane. In order to prevent malfunctions or attacks at the control plane and its propagation to the data and application planes, it becomes mandatory to empower the control plane with resilience and security properties. Consequently, the resilience of critical nodes in SDN/NFV such as the SDN controllers, the VIM, the VNFMs, and the NFVO is a very hot topic in research. In the sequel, we describe two ways to mitigate the issues previously described and ensure the security and resilience of critical nodes of a softwarized network.

1) Cross-layer fault management: Fault management operations (fault-detection, fault-diagnosis, and fault-recovery) ensure the service delivery at both at design and at operation stages and its goal is to provide resilience. This phase depends on metric identification, data collection, correlation, and analytics.

a) Metrics identification: it concerns the identification of the appropriate metrics and Key performance Indicators (KPI) that may give relevant insight on the behavior of both the infrastructure and overlying services. These metrics are defined at different layers: NFVI, VMs, hypervisor, virtualized layer, and service layers. Examples of metrics in SDN are the control session capacity of the SDN controller or the forwarding table capacity of SDN controller.

b) Data collection, correlation, and analytics: this concerns the retrieval and aggregation of the data from the different management and control entities in the SDN/NFV infrastructure.

2) Learning dynamic resource dependencies: A key challenge to correlate alarms in SDN/NFV is to build a network model encompassing the infrastructure (1), the deployed services (2) and the mapping of the virtual resources on the infrastructure (3), as shown in Figure 5, where the mapping of services is dynamic because each virtual link connecting VNFs depends on a path composed of a set of resources chosen by the SDN controller. Generating this model at run-time, in an automated manner and maintaining it updated by learning the dependencies of newly added resources is a challenging task. However, a topology-aware fault management mechanism only takes into account faults seen in the topology, whilst a service-aware mechanism also considers how faults propagate to the service layer. This work [13] proposes both a topology and service aware correlation mechanism for SDN/NFV dynamic environments.

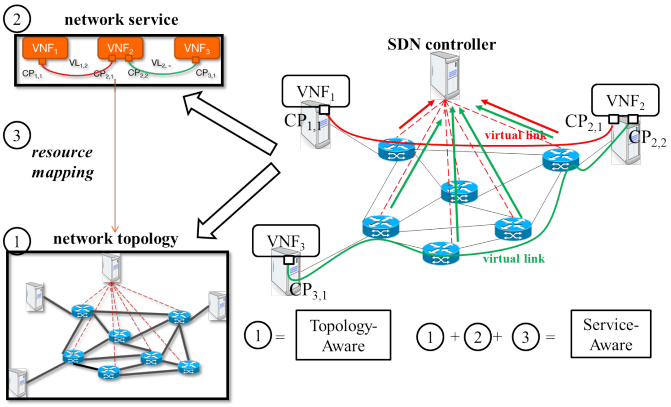

Fig. 5. Resource dynamicity in SDN/NFV

D. Network Slices

5G network will be a multi-slice network to cover the diverse defined use cases [10]. We will have a set of verticals who use a set of network slices composed of virtual resources which are mapped onto the physical infrastructure in a certain manner. Consequently, the network security and resilience level depends on the slices security and resilience level. This latter is based on three factors. Obviously, a slice security and resilience is firstly build upon the way the virtual resources are mapped on the physical infrastructure. Any unavailability or failure of the physical layer impacts an unbounded number of overlying virtual resources. As a result a large number of slices, services and end-users can be impacted. This effect is known as fault propagation effect. Then, slice security and

resilience relies on how are shared the network resources between slices and how the isolation is maintained. Indeed, isolation vulnerabilities in physical or virtualized layers can lead to the propagation of attacks between slices sharing network resources or communicating together. This is known as cascade effects. Finally, as in 5G, MNOs may enable verticals to manages their slices through APIs or portals. It is of interest to secure this access as it presents a new attack vector to slices. A vertical must be able to manage and get data only about its associated slices.

The security and resilience issues described previously (i.e., Physical layer failure, slice isolation and API attacks) can be mitigated by computing redundancy in real-time,in different locations, different physical machines, or virtual machines, which is not possible in traditional static networks, however, it should be feasible in SDN/NFV based networks. Hence, MNO can preallocate simultaneous and disjoint backup paths and active paths at a given layer to avoid simultaneous failures in both paths.

VII. Privacy and Regulation Management

Privacy concerns are becoming of main interest especially after the multiple recent attacks [14]. Therefore, 5G networks should be more careful about privacy issues. 5G privacy level must be higher to current mobile network privacy level. In addition, 5G network, like the current mobile network generations, must undergo a set of regulations including new and old ones.

A. End User Privacy

In mobile networks, We can distinguish two areas where scientists should have further considerations about privacy: (i) User identifiers (i.e., IMSI, IMEI) and (ii) user data (i.e., data exchanged during communications).

Current mobile networks are designed in such a way that identifiers are not protected in some cases such as the first Attach Request or identities request. The identifiers disclosure enables various location privacy attacks like illegitimate device and user tracking and monitoring. In order to mitigate this issue, current mobile networks propose the use of temporary identifiers (e.g., TMSI, GUTI). However, this solution has two main limitations. First, there is no requirement about the randomness of this temporary identifiers. Second, this solution protects only against passive attackers. An active attacker can force the network to send the identifier in plain text [15]. Known that many solutions have been proposed in the literature [15], [16], [17], [18], this privacy issue should be mitigated at the design of 5G.

Regarding the user data protection, current mobile networks propose an encryption service (i.e., communication encryption). However, only link-encryption (i.e., intermediate network nodes are expected to decrypt coming flows and encrypt outgoing ones) has been provided. In such a case, end-users have no insurance about the confidentiality of their data. Indeed, only a faulty node can enable for instance an unauthorized exposure of users' communications. That's why, 5G networks should provide end-to-end encryption as a basic network function in order to not only protect users' privacy, but also, to enable lawful intercept while preserving backward and forward secrecy of users' communications. Such solution could be based on cryptographic mechanisms like attribute based encryption or threshold systems.

Introducing encryption in mobile network will also bring a new challenge. Indeed, legitimate security monitoring services must adapt its techniques and algorithms to instead study encrypted flows. This can be achieved by homomorphic algorithms. However, its efficiency still needs improvement to be considered in realistic environments.

B. Lawful Interception

Lawful Interception (LI) [19] is a legal obligation for MNOs. Regardless the mobile network generation or the ecosystem structure, LI requirements remain the same. Indeed, the LI dilemma is ensuring the end user and services privacy (namely the confidentiality) vice versa the ability to answer any LI request. This mainly results in the following elements. The MNO must ensure that only those under surveillance are wiretapped, e.g., authorities cannot wiretap users/entities not on the list. Only the MNO must be able to trigger a Lawful interception. These imply a strong isolation requirement in the mobile network to prevent fraudulent network access and abusive use of resources. In addition, only concerned entities (i.e., the MNO LI service and Law Enforcement Agency) have access to the list of the wiretapped and collected data. The MNO must be able to answer any LI request without requiring any third party. This operation must not be detectable through observation or quality of service. Finally, in case of an end-to-end encryption managed by the network, the MNO should be able to deliver plain data or the encrypted data along with the decryption key.

C. Network Neutrality

The 5G is assumed to be the future Internet. Unlike the current mobile network generations, so called 4G/LTE, that provides homogeneous connectivity to customers, 5G is expected to be versatile: it will encompass various access network technologies, i.e., fixed access, radio access (3GPP RANs and Non-3GPP RANs), and provide connectivity to heterogeneous services such as mass market, IoT and Public Safety. In this context, the telecom Industry warns, in what they called 5G Manifesto, that the current Net Neutrality guidelines, as put forward by BEREC, create significant uncertainties around 5G return on investment, concurs with Industry verticals that the implementation of Net Neutrality Laws should allow for both innovative specialised services required by industrial applications and the Internet Access quality expected by all consumers, and points out the danger of restrictive Net Neutrality rules.

VIII. Related work

5G-ENSURE project is an European project part of the 5G-PPP consortium. It aims at addressing priorities for security

and resilience in 5G networks. 5G-ENSURE provides the following contributions:

- a set of 5G use cases relevant to security, privacy and resilience [20],
- a draft of a trust model [21] for multi-party operated services,
- a draft of a threat analysis [22] for all the described use cases,
- a draft describing a 5G Security architecture [23],
- a set of enablers mitigating security, privacy and resilience challenges [24], and,
- the first 5G testbed following the DevOps principles to deploy the enablers [25].

In the same direction, 5G-PPP published a whitepaper in the latest Mobile World Congress 2017 [26], where a high level overview about the achievements of 5G-PPP phase-I project, was proposed. The whitepaper describes four main topics: (i) the potentials transformation of the mobile network ecosystem, (ii) the new possible architecture to have enhanced performance, hence, a better user experience, (iii) the key requirements to have a secure, reliable and flexible 5G network and, (iv) some recommendations about deployment, standardization and regulation.

5G standardization is indirectly associated to many standardization organizations such as ETSI, NGMN, ITU, 3GPP, etc. However, it is still mainly standardized by 3GPP [27]. In 3GPP, the studies started in 2015 by collecting the potential 5G requirements. These requirements are now consolidated in the Technical Specification (TS 22.261 [28]) that will be the input of further studies.

In the literature, to the best knowledge of the authors, only Schneider and Horn proposed a recent study about 5G security challenges [29]. Usually, scientists focus on a specific problem such as privacy mechanisms [15], [16], [17], [18], NFV related security and resilience [30], [31], [32] or SDN related security and resilience [33], [13], [31]. However, the authors of [29] presented a high level security insight on the requirements and discussed the security challenges that current security mechanisms cannot overcome in the 5G context. We rather propose a 5G Network implementation based on SDN/NFV, detail its associated challenges in terms of security, resilience, trust and privacy, and provide some directions to overcome these challenges.

IX. Conclusion

5G seems to be adopting new multi-party based ecosystems where several actors may be cooperating in the service delivery. This will imply the use reputation and trust mechanisms able to somehow quantify which actor is financially responsible for the service outages or degradations. In addition, 5G will strongly rely on new network paradigms, i.e., softwarization (SDN, NFV, and slicing). Softwarization brings several challenges into the table. There is a need to manage and ensure the security and resilience of critical software entities while taking into account the dynamicity of those softwarized infrastructures. To this end, we need intelligent fault management and mitigation risk strategies to act on the network at design time and run-time. Softwarization raises issues about the importance of a strong network authentication and strong slices isolation. Finally, 5G networks as its predecessors must undergo a set of regulations whilst ensuring users privacy.

Acknowledgment

This research was partly performed within the 5G-ENSURE project (www.5GEnsure.eu) the EU Framework Programme for Research and Innovation Horizon 2020 under grant agreement no. 671562

References

[1] Google, "Consumer barometer with google," https://www.consumerbarometer.com/en/insights/?countryCode=GL.

[2] M. E. Porter, "How Competitive Forces Shape Strategy," *Harvard Business Review*, vol. 57, no. 2, 1979.

[3] 5GPPP, "5G Infrastructure Public Private Partnership (5GPPP) the next generation of communication networks and services," http://superfluidity.eu/wp-content/uploads/5GPPP-brochure-draft02.pdf.

[4] "H2020 METIS Project," https://www.metis2020.com/, 2013-2015.

[5] METIS Project, "Deliverable D1.1 Scenarios, requirements and KPIs for 5G mobile and wireless system ," https://www.metis2020.com/wp-content/uploads/deliverables/METIS_D1.1_v1.pdf, 2013.

[6] ONF (Open Networking Foundation), "Software-Defined Networking (SDN) Definition," https://www.opennetworking.org/sdn-resources/sdn-definition.

[7] ——, "SDN Architecture Overview, Version 1.0," https://www.opennetworking.org/images/stories/downloads/sdn-resources/technical-reports/SDN-architecture-overview-1.0.pdf, december 2013.

[8] ETSI GS NFV 002 V1.1.1(2013-10)), " Network Functions Virtualisation (NFV); Architectural Framework ," http://www.etsi.org/deliver/etsi_gs/nfv/001_099/002/01.01.01_60/gs_nfv002v010101p.pdf.

[9] "European Telecommunications Standards Institute," http://www.etsi.org/.

[10] NGMN Alliance, " 5G White Paper ," https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf, March 2015.

[11] ETSI NFV Group Specification Draft, " Network Functions Virtualisation (NFV); Ecosystem; Report on SDN Usage in NFV Architectural Framework ," http://www.etsi.org/deliver/etsi_gs/NFV-EVE/001_099/005/01.01.01_60/gs_NFV-EVE005v010101p.pdf, December 2015.

[12] E. G. N.-S. . V1.1.1, *Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance* , http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/003/01.01.01_60/gs_NFV-SEC003v010101p.pdf, December 2014.

[13] J. M. Sánchez, I. G. B. Yahia, and N. Crespi, "Self-modeling based diagnosis of services over programmable networks," in *2016 IEEE NetSoft Conference and Workshops (NetSoft)*, June 2016, pp. 277–285.

[14] James Ball, The Guardian, "The NSA Monitored The Phone Calls Of 35 World Leaders." [Online]. Available: http://www.businessinsider.com/nsa-phone-calls-world-leaders-2013-10?IR=T

[15] F. van den Broek, R. Verdult, and J. de Ruiter, "Defeating imsi catchers," in *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '15. New York, NY, USA: ACM, 2015, pp. 340–351. [Online]. Available: http://doi.acm.org/10.1145/2810103.2813615

[16] P. Ginzboorg and V. Niemi, "Privacy of the long-term identities in cellular networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, ser. MobiMedia '16. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 167–175. [Online]. Available: http://dl.acm.org/citation.cfm?id=3021385.3021416

[17] K. Norrman, M. Näslund, and E. Dubrova, "Protecting imsi and user privacy in 5g networks," in *Proceedings of the 9th EAI International Conference on Mobile Multimedia Communications*, ser. MobiMedia '16. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2016, pp. 159–166. [Online]. Available: http://dl.acm.org/citation.cfm?id=3021385.3021415

[18] A. Dabrowski, N. Pianta, T. Klepp, M. Mulazzani, and E. Weippl, "Imsi-catch me if you can: Imsi-catcher-catchers," in *Proceedings of the 30th Annual Computer Security Applications Conference*, ser. ACSAC '14. New York, NY, USA: ACM, 2014, pp. 246–255. [Online]. Available: http://doi.acm.org/10.1145/2664243.2664272

[19] 3GPP TS33.106, "3G security; Lawful Interception requirements (Release 13)," Dec 2015. [Online]. Available: http://www.3gpp.org/DynaReport/33106.htm

[20] 5G-ENSURE, *Deliverable D2.1: Use Cases*, http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.1-UseCases.pdf, February 2016.

[21] ——, *Deliverable D2.2: Trust model (draft)*, http://www.5gensure.eu/sites/default/files/5G-ENSURE_D2.2%20Trust%20model%20%28draft%29_v1.1.pdf, November 2016.

[22] ——, *Deliverable D2.3: Risk Assessment, Mitigation and Requirements (Draft)*, http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.3-RiskAssessmentMitigationRequirements.pdf, August 2016.

[23] ——, *Deliverable D2.4: Security Architecture (draft)*, http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D2.4-SecurityArchitectureDraft.pdf, October 2016.

[24] ——, *Deliverable D3.2: 5G-PPP security enablers open specifications (v1.0)*, http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D3.2-5G-PPPSecurityEnablersOpenSpecifications_v1.0.pdf, June 2016.

[25] ——, *Deliverable D4.1: 5G Security testbed architecture*, http://www.5gensure.eu/sites/default/files/Deliverables/5G-ENSURE_D4.1-5G_Security_testbed_architecture_v1.0.pdf, June 2016.

[26] 5G-PPP whitepaper, "5G Innovations for new business opportunities ," *Mobile World Congress*, 02 2017.

[27] The 3rd Generation Partnership Project (3GPP), "The Mobile Broadband Standard." [Online]. Available: http://www.3gpp.org/about-3gpp

[28] 3GPP TS22.261, "Service requirements for the 5G system;Stage 1 (Release 15)," Mar 2017. [Online]. Available: https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107

[29] P. Schneider and G. Horn, "Towards 5g security," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug 2015, pp. 1165–1170.

[30] R. Mijumbi, J. Serrat, J. L. Gorricho, N. Bouten, F. D. Turck, and R. Boutaba, "Network function virtualization: State-of-the-art and research challenges," *IEEE Communications Surveys Tutorials*, vol. 18, no. 1, pp. 236–262, Firstquarter 2016.

[31] D. V. Bernardo and B. B. Chua, "Introduction and analysis of sdn and nfv security architecture (sn-seca)," in *2015 IEEE 29th International Conference on Advanced Information Networking and Applications*, March 2015, pp. 796–801.

[32] B. Jaeger, "Security orchestrator: Introducing a security orchestrator in the context of the etsi nfv reference architecture," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, Aug 2015, pp. 1255–1260.

[33] S. Scott-Hayward, G. O'Callaghan, and S. Sezer, "Sdn security: A survey," in *2013 IEEE SDN for Future Networks and Services (SDN4FNS)*, Nov 2013, pp. 1–7.