IEEE Open Journal of the Computer Society

IEEE Xplore Digital Library
http://ieeexplore.ieee.org/Xplore

Towards Secure and Intelligent Network Slicing for 5G Networks

Fatima Salahdine*, Qiang Liu, Tao Han
Corresponding author: fsalahdi@uncc.edu

***Abstract*—Network slicing is one of the emerging technologies allowing resource sharing among different network entities in 5G networks. It enables delivering smart, critical, and multi-services with distinctive requirements transiting from network as an infrastructure to network as a service setup. Although its advantages, it is facing several challenges raised from isolation and resource sharing among services leading to security issues. Security is a critical problem for network slicing as slices serving customized services with different requirements may also have different security levels and policies. Thus, considering the impact of these security issues on network slices is required when defining and designing security protocols. Addressing these challenges is necessary to protect users' security and privacy while maintaining the required performance and quality of service. Most of the existing works covered only one or more aspects of the network slicing including, architecture, taxonomy, challenges, security issues, attacks classification, possible solutions, and future scope. In this paper, we extensively investigated all these aspects and others, we analyzed how the security can be ensured inside and outside of the network slices with resource isolation, machine learning, and cryptography with an end to end security. We presented a deep review of the security issues threatening the network slicing and how to mitigate them over a multi-domain infrastructure in 5G networks. we evaluated the performance of some of these solutions in preventing malicious attacks through experiments using Open Air Interface.**

***Index Terms*—5G networks, security, network slicing, resource management, orchestration, isolation, artfificial intelligence**

I. Introduction

IN the last decades, a number of new technologies have been developed to ensure high quality of service (QoS) in wireless networks. These technologies increased the demand on radio resources in terms of bandwidth and frequency spectrum. Existing wireless networks cannot satisfy today's network requirements with limited resources. Therefore, a transition to a new approach with dense and flexible architecture is a must to maintain the required QoS and quality of experience (QoE) while saving resources [1]. Researchers focused on developing advanced solutions to effectively satisfy each service's requirements no more no less with efficient resource management increasing the network throughput and decreasing the traffic load. Recent emerging technologies open up new services with diverse specifications and requirements to be hosted without assigning extra resources while maintaining network performance [2].

Fatima Salahdine is with the Department of Electrical and Computer Engineering, University of North Carolina at Charlotte. Qiang Liu is with the School of Computing, University of Nebraska - Lincoln, Tao Han is with the Helen and John C. Hartmann Department of Electrical and Computer Engineering at New Jersey Institute of Technology

Network slicing has been proposed as a low-cost solution to deliver multiple customized services with diverse requirements over a single network [3]. It enables new services in multiple logical networks over common physical infrastructure allowing different services with specific requirements. Over the physical infrastructure, several logical networks are created to support distinctive services per slice. For instance, the network can support several slices including smart agriculture slice, smart building slice, smart grid slice, smart health care slice, smart forest surveillance slice, augmented reality slice, smart transportation slice, and smart seaport slice [4].

This network architecture aims at ensuring service availability on users' demand with infrastructure virtualization, slice instantiation, and resource orchestration [5]. It performs via network function virtualization (NFV), software defined networking (SDN), mobile edge computing (MEC), and cloud computing. NFV allows using generic hardware for efficient network function implementation with low cost. SDN allows separating the control plane from the data plane for efficient and flexible resource management. Network slicing based NFV and SDN are necessary technologies for 5G and beyond. They will boost the communication market by allowing communication technologies to penetrate the industry with dedicated services as network-as-a-service (NaaS) and network-as-a-platform (NaaP) services. They will provide industries with more flexible deployment to implement their services while optimizing resources. Service providers operate multiple slices in parallel to host numerous companies and ensure their proper isolation.

This technology has been applied into several domain in addition to the 5G networks, including smart transportation systems, smart grid, smart homes, smart industry, and smart health care. Smart homes are used to provide state-of-the-art control and automation facilities, such as smart security, smart elevators, and smart plug-in hybrid electric vehicle charging. Smart grids use information and communication technologies with emerging computing technologies for the transformation of conventional grids to offer reductions in global warming, operational expenditure, and smart meters. In smart health care, network slicing enables real time health care facilities with low cost and high efficiency, including remote surgery.

Boosted by the integration of new key technologies, network slicing allows transiting from static to more dynamic network by building multiple virtual networks serving multiple advanced services with diverse requirements. It enables functional and infrastructural sharing among slices to deliver distinctive services with low resource consumption at low

Digital Object Identifier 10.1109/OJCS.2022.3161933

cost. Despite these advantages and others, resource sharing raised several concerns and security issues, which requires more attention to figure out how to adopt network slicing while maintaining high security level in dynamic and multi-tenant environments. Network slicing is facing a number of challenges for full isolation while sharing radio resources for customized services [6], [7]. Using network slicing in radio access network (RAN) involves separating resources leading to high spectrum usage. Moreover, security requirements differ among slices and tenants per service, which opens the door to several threats coming from less secure slices targeting slices with critical services.

A number of research papers investigated the network slicing have been published in the recent years. These papers can be classified according to how they treated the network slicing and the security concerns, namely (i) review of network slicing and the theory behind it with no security considerations [8]–[14]; (ii) focus on security and only referred to network slicing [15], [16]; (iii) focus on network slicing and the security threats introduced by the network slicing [17]–[19]; and (iv) focus only on security in network slicing [20], [21].

For instance, the authors presented a comprehensive review on network slicing without taking into account the taxonomy of the different approaches and the security concerns [8]. In [9], the authors discussed some network slicing open issues related to resource management and orchestration. In [10], the authors presented a comprehensive survey where they covered several network slicing aspects including requirements and challenges, but security issues were not discussed. In [11], the authors briefly investigated network slicing from layer's perspective, while some other papers focused on only one perspective: domain, plane, or layer [12]. Some other papers focused on how network slicing can be enabled with NFV and SDN with no review about security issues [13]. In [14], the authors reviewed the network slicing concept and discussed some of its applications and use cases.

In [15], [16], the authors reviewed the 5G security and privacy and their associated threats. They only mentioned network slicing as one of the 5G key technologies. In [17], the authors briefly discussed some of the security attacks targeting the network slicing and their impact on the security requirements. They also investigated a number of defense strategies to address these security attacks. In [18], [19], the authors presented a brief systematic review of the security issues introduced by the network slicing. The security architecture dedicated to the network slicing has been reviewed based on different perspectives, including 3PP specifications and 5G PPP [16]. In [20], the authors presented an extensive overview of the network slicing security and discussed the security issues related to network slicing. They only provided the literature review, but they did not discuss the possible solutions to enforce the slices security or experimentally verify their performance. In [21], the authors presented a brief state of the art of the network slicing security and discussed some of the possible solutions for future investigation.

Moreover, several approaches have been proposed to enhance the security of the network slicing [22]–[25]. For instance, an automated framework has been proposed based on the intent-based networking (IBN) for end-to-end (E2E) slicing configuration and management over access and core networks allowing flexible and customized services deployment [22]. It has been implemented using generative adversarial networks (GAN) deep learning algorithm to automate the different processes involved in the slice life cycle including creation, configuration, management, and resource consumption and prediction [23]. In [24], the authors investigated how trust zones can enhance network slicing security as they may perform as alternative solutions to create protected logical networks with critical elements of the slice. In [25], the authors proposed an authentication framework based on Diffie-Hellman key agreement to enable IoT services under 5G infrastructure in order to support the network slicing security. The proposed framework allows securing the access to the IoT services by enforcing key negotiation by the involved servers and users.

Table.I compares the discussed research papers and highlights the added value introduced by this paper. Most of the conducted research is fully dedicated to network slicing by covering its terminology, concepts, and resource sharing in 5G systems. Security issues introduced by the network slicing were outside of the scope of their works. Other papers discussed some of the security issues and investigated how they can be addressed through isolation with no experiments simulations. Therefore, there are very limited contributions in securing network slicing for 5G networks, which requires more investigation. Thus, there is a great need for a deep review of network slicing from recent advances to open issues with focus on security. This paper aims at extensively covering most of the important aspects of the network slicing as well as its security in one single work. It evaluates the performance of the security solutions through experiments using open air interface. To our knowledge, there is no extensive review paper on network slicing and security considering experimental evaluation. This paper represents examples of results for uplink and downlink communications to prevent malicious attacks with isolation and artificial intelligence based solutions.

In this paper, we investigated the recent advances of network slicing and we classified its architecture according to which perspective is considered. We classified different attacks targeting network slicing into three main classes: inter, intra, and life cycle attacks. We analyzed how these attacks can be mitigated and we evaluated the performance of some of them using Open Air Interface. We discussed the research challenges with future scope for network slicing implementation in 5G systems.

The rest of the paper is organized as follows: Section II represented an overview of network slicing theory while Section III represented the security concerns and attacks classified according to which security level is targeted. Section IV discussed how network slicing can be protected and how these attacks can be mitigated. We implemented some of these security solutions for performance evaluation. Section V discussed the open issues facing the network slicing security for future directions. Finally, a conclusion is given at the end.

Table.II represents a list of the abbreviations used in the paper with their corresponding definition.

TABLE I: Comparison

References	Network slicing	Security	Network slicing security	Attacks	Solutions	Experimental Evaluation
[8]	✓✓	x	x	x	x	x
[9]	✓✓	x	x	x	x	x
[10]	✓✓	x	x	x	x	x
[11]	✓✓	x	x	x	x	x
[12]	✓✓	x	x	x	x	x
[13]	✓✓	x	x	x	x	x
[14]	✓✓	x	x	x	x	x
[15]	✓	✓✓	x	x	x	x
[16]	✓	✓✓	✓	x	x	x
[17]	✓✓	x	✓	✓	✓	x
[18]	✓	x	✓✓	x	x	x
[19]	✓	x	✓✓	x	x	x
[20]	✓	x	✓✓	✓✓	x	x
[21]	x	x	✓✓	✓✓	✓	x
Our paper	✓✓	✓✓	✓✓	✓✓	✓✓	✓✓

✓: brief ✓✓: extensive

II. Network slicing

A. Overview

The rapid evolution and development of the wireless communication systems demand several services, applications, and scenarios, namely enhanced mobile broadband (eMBB), ultra-reliable and low-latency communication (uRLLC), and massive machine type communication (mMTC). eMBB services require high throughput such as virtual reality and video streaming. uRLLC services are critical services requiring very low latency and low minimal errors such as autonomous driving. mMTC services are high connectivity services delivered to a high number of devices and users such as sensing and monitoring devices. These services cannot be fit in the current network, which requires one network fitting all.

Network slicing has been proposed in 5G networks to allow delivering customized services with different requirements over one single network. Fig. 1 illustrates how the network slicing framework can perform several services simultaneously with access, transport, and core network slices [26]. Core network slice includes both control plane and user plane with shared and non-shared functions among slices. Examples of these functions include session management function (SMF), mobility management function (MMF), user plane function (UPF), and policy control function (PCF). Several companies proposed and designed their own network slicing systems to perform their industry including Ericsson and Nokia [19].

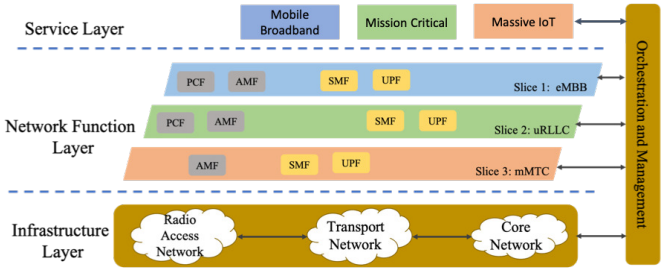

Fig. 1: Network slicing.

Network slicing has been proposed as a new paradigm to enable infrastructure sharing among services, customers, and providers. It allows creating several logical networks over one physical infrastructure to deliver services with diverse characteristics to simultaneously satisfy multiple technologies. 5G, 6G, and beyond are expected to offer a variety of customized services with specific requirements in security, reliability, data rate, latency, resources, and cost. Assigning each service with particular needs enhances the network performance than providing unnecessary resources. Services differ from each other, some services require low latency and high speed, or high throughput and tolerable latency, or high security level with tolerable data rate and latency.

Network slicing management involves a number of components enabling virtual and physical resource management: NFVs, SDN controllers, and orchestrators [27]. NFVs refer to cloud-based functions deployed to define each slice requirements and characteristics. SDN controllers receive commends from the orchestrator to create slice instances by connecting virtual functions by SDN networks [28], [29]. Orchestrators allow automating cross domain resource management and configuration inter-slices and intra-slices by automating services creation, deployment, and resource monitoring within slices.

There are two types of orchestrators: service orchestrator (SO) and resource orchestrator (RO). SOs create and manage multiple services between NFVs while ROs coordinate and manage NFVs resources. Examples of open-source network slicing orchestrators include OSM, openMANO, openNFV, openBaton, openFV, ZooM, SliMANO, ONAP, OpenBaton, JOX, cloudNFV, Cloudify, and FlexRAN [27], [30]. These solutions have been developed by different companies to slice and manage their resources in access, core, and transport networks. An end-to-end network slicing orchestrator has been developed to slice resources in the three network domains [31]. It has been evaluated with real hardware implementation to demonstrate its performance in providing good resource isolation per slice. Three scenarios have been considered: eMBB slice for organizing a sport event in a stadium with audience, mMTC slice for power meter reading scenario, and URLLC slice for performing remote surgery. It is a Huawei based infrastructure with NFVs controllers, SDN controllers, and orchestrators.

TABLE II: List of abbreviations

Abbreviation	Definition
QoS	Quality of Service
QoE	Quality of Experience
API	Application Programming Interface
NS	Network Slicing
NFV	Network Function Virtualization
SDN	Software Defined Networking
MEC	Mobile Edge Computing
NaaS	Network-as-a-Service
NaaP	Network-as-a-Platform
RAN	Radio Access Network
IBN	Intent-Based Networking
E2E	End-to-End
GAN	Generative Adversarial Networks
eMBB	Enhanced Mobile Broadband
uRLLC	Ultra- Reliable And Low-Latency Communication
mMTC	Massive Machine Type Communication
SMF	Session Management Function
MMF	Mobility Management Function
UPF	User Plane Function
PCF	Policy Control Function
SO	Service Orchestrator
RO	Resource Orchestrator
NSI	Network Slicing Instance
NSSI	Network Slicing Subnet Instance
NSS	Network Sub-Slice
NST	Network Slicing Template
MF	Management Function
CSMF	Communication Service Management Function
NSMF	Network Slice Management Function
NSSMF	Network Slice Subnet Management Function
PNF	Physical Network Functions
VNF	Virtual Network Functions
RNF	Resource Network Functions
DoS	Denial of Service
DDoS	Distributed Denial of Service
TLS	Transport Layer Security
O-Auth	Open Authorization
MPLS	Multi-Protocol Label Switching
IoE	Internet of Everything
IDS	Intrusion Detection Systems
OSINT	Open-Source Intelligence
FIFO	First-Come-First-Out
NORMA	Novel Radio Multi-Service Adaptive Network
MANO	Management and Orchestration
AI	Artificial Intelligence

A network slicing is a logical network built over the shared physical infrastructure, which includes the radio access network, core network, cloud, edge computing nodes, unmanned aerial vehicles, and satellites [32]. Network slices are created on demand, isolated in terms of performance and resources, and independent in terms of control and management. The business model of the network slicing involves several elements and entities with specific roles and capabilities. These elements are network slicing instance (NSI), network slicing subnet instance (NSSI), logical network, network sub-slice (NSS), network slicing template (NST), network segment, NFV, SDN, network slicing manager, communication service manager, resource slice, network slicing provider, network slicing terminal, network slicing tenant, network slicing repository, slice border control, slice selection function, infrastructure owner, infrastructure slice, infrastructure slice provider, and infrastructure slice tenant. NSI refers to a set of end-to-end logical networks providing multiple services with customized requirements. It includes multiple sub-slice instances. NSSI refers to the local logical network inside a network slice, which can be shared between multiple NSIs.

Logical networks refer to virtual network function instances created on the top of a single physical network. Indeed, network slicing is the logical network created after slicing the physical network into multiple virtual networks. Logical network offers specific services requirements requested by the customer on demand. A network slicing can be divided into several NSS. Network slicing template (NST) describes in detail the creation of a slice in terms of structure, configuration, design, components, and requirements. A slice will be then created based on the template. Network segment is the portion of the network with common features. NFV is based on generic hardware for network functions implementation. SDN consists of separating the control plane from the data plane for easier network management. For network slicing manager, each slice or sub-slice has its own network slice manager to manage its life cycle through multiple management functions, namely communication service management function (CSMF), network slice management function (NSMF), and network slice subnet management function (NSSMF) [9]. These functions aim at managing the life cycle of a service and interacting with the network slice manager. CSMFs manage, communicate, and update the slice requirements to support the services requests via communication service manager. NSMFs manage the NSIs based on the received CSMFs notifications. NSSMFs manage the NSSIs according to the NSMF requirements.

Communication service requirements are translated to network slicing requirements by the CSMFs while resource orchestration and life cycle management are performed by the NSMFs. Network slicing requirements include network type, network capacity, QoS, delay, security level, number of devices, and throughput. Resource slice refers to physical and virtual resources required by the network slices to operate. Network slicing provider is the owner of the physical infrastructure where multiple slices are built. Network slicing terminal is a cognitive device aware of the network slicing concept.

Network slicing tenants are the NSI users delivering certain services requested by customers. Network slicing repository includes active slices with their characteristics. Slice border control allows users to slice attachments while slice selection function allows them to join a slice. Infrastructure owner is the physical infrastructure owner. Infrastructure slice is all the different types of infrastructure required to meet the services requirements. Infrastructure slice provider is the infrastructure

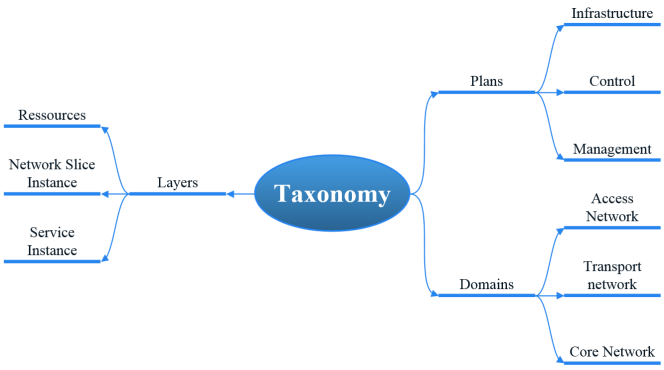

Fig. 2: Network slicing taxonomy.

owner leasing the infrastructure for hosting diverse services through network slicing. Infrastructure slice tenants are the infrastructure slice users.

B. Architecture

Network slicing architecture can be seen from several perspectives: domain, plan, and layer, as illustrated in Fig. 2. From the domain perspective, network slicing performs over three domains or sub-slices: radio access, transport, and core networks. For RAN sub-slice, end-to-end slicing requires sliceable and isolated RAN with resource allocation and scheduling. Assigning a specific spectrum to slices requiring high level of security represents more security challenges. Network slicing has been adopted for physical and virtual resource management including physical and virtual network functions (PNF,VNF). PNF refers to the hardware resources while VNF refers to the functions and the protocols. For transport sub-slice, it corresponds to the transport path used to connect core sub-slices to external networks with SDN through physical and virtual routers. For core sub-slice, it corresponds to a virtual core network over NFV architecture for customized services with flexible and scalable resource allocation [33]. It is instantiated with a slice template and connected to corresponding RAN sub-slices. It includes common and special network functions. Common network functions are shared among service infrastructure while special network functions are dedicated to specific service infrastructure.

From the plane perspective, network slicing performs over three main plans: infrastructure, control framework, and management planes. Infrastructure plane includes physical and virtual resource while control framework includes slice controllers placed in each domain for security and service requirements by each service provider. Management plane refers to orchestrators receiving and performing business orders for several purposes, including slice creation, slice deletion, resource allocation, and parameters adjustment. Orchestrators manage and respond to these orders by sending real time reports about resource usage and slice instance.

On the other hand, network slicing architecture involves three main layers with independent management functions (MFs), namely resource, network slice instance (NSI), and service instance layers. Each network slice layer is associated with its own management functions: communication service management function (CSMF), network slice management function (NSMF), and resource management function (RMF). Resource layer is the lower layer defining the required resources to provide on-demand services to customers over one or several NSIs. It is associated with the sharing or dedicating RMFs. These resources are physical and logical network resources and network functions including storage, processing, switching, routing, authentication, and resource management functions. NSI layer is the middle layer defining slices with their specific requirements demanded by the service instance. It includes network functions and resources to run them. A slice can serve one or more service instances over common or different physical infrastructures using distinct or shared resources. Service instance layer is the upper layer defining the service instances offered to the end users over the slices.

C. Slice life cycle

Slice life cycle involves four stages: preparation, commissioning, operation, and decommissioning.

- Preparation: It prepares the network environment for new slice creation or modification by performing several actions including slice building and template definition. Slice building consists of building the network environment and the required resources to create the slice. Template definition consists of clearly writing down the specific requirements for each slice owner at its request. Examples of preparation tasks include service-level agreement (SLA) decomposition and slice type classification. At this stage, the slice is not created yet.
- Commissioning: At this stage, several actions are processed to build the slice including instantiation, configuration, and activation. Instantiation consists of instantiating the slice by building it from a defined template with specific instance information and performance requirements. Configuration consists of configuring the parameters and creating the resources required by the slice to satisfy the service requirements. Activation consists of installing and activating the slice to be ready for service. Examples of commissioning tasks include customization of slice functions. At this stage, the slice is created but not in use yet.
- Operation: At this stage, the created slice is in use to serve customized services for multiple customers with specific requirements. Several actions are processed at this stage, namely modification, supervision, and reporting. Modification consists of upgrading or changing the slice configuration and requirements in terms of associated resources and network functions. Supervision consists of monitoring the slice to ensure its well-functioning. Reporting consists of reporting any problem related to the slice performance for troubleshooting. At this stage, the slice is in use.
- Decommissioning: At this stage, the slice is no longer in use and needs to be deleted by freeing the assigned storage and resources. Several actions are processed at this stage, namely deletion, deallocation, and destruction. Deletion consists of deleting the slice completely at the

request of its owner or after finishing the service. Deallocation consists of deallocating the associated resources and network functions. Destruction consists of destroying all the data and the sensitive information used by the services as well as the customer's details. At this stage, the slice does not exist anymore.

The life cycle stages are controlled by the slice manager by performing a number of actions, namely slice creation, slice destruction, resource allocation, resource deallocation, and parameters configuration [34].

D. Differences between network slicing in 5G and B5G

Network slicing in 5G networks is facing a number of challenges and issues including security issues, high expenditure, heavy computing, and high energy consumption. Managing massive number of slices demands heavy computing, which limits the network slicing efficiency [35]. Network slicing is expected to support the newly emerging applications and requirements of the beyond 5G networks (B5G), which refers to deep slicing [35], [36]. B5G systems are expected to offer new advanced services while supporting the network services eMBB, URLLC, and mTCM through network slicing. As ultra-dense heterogeneous networks, B5G networks are expected to be more complex, which requires smart and advanced architecture with high learning capabilities to make decisions and adapt to the service requirements. 5G network slicing is a static and per service network, which cannot meet the B5G requirements in terms of user mobility and unexpected service utilization [37], [38].

The demand for resources per each slices is then changing spatio-temporally according to the network load, QoS requirement, user mobility, resource needed, and service utilization. New emerging technologies will be applied to meet the B5G requirements including edge AI, collaborative learning, distributed learning, and federated learning. Edge AI refers to applying AI at the edge devices [39]. As a distributed learning, federated learning allows training with sensitive data from collaborating clients without sharing these data among them [40]. It allows preserving the clients privacy while exchanging only the learning results. Deep slicing combines the advantages of network slicing with the distributed learning to secure and protect the users data. Deep slicing requires high cost for deployment. These difference between the network slicing in 5G and B5G networks impose the necessity of designing new dynamic and flexible architecture taking into account the dynamic nature of the future networks. In [38], a per user basis network slicing, user-oriented network slicing architecture (UONA) has been proposed to offer personalized and diversified services that meet personal requirements of users. It required a new signaling protocol to avoid scalability issues by brokering among users.

III. Network slicing security

Security is one of the critical issues facing the network slicing as it provides diverse services with different security requirements [41]. When serving multi-domain infrastructures with multiple services for several customers, security problems become stronger and more complex. Moreover, security issues raised when sharing resources among slices from services of different security policies defined by distinctive verticals and operators. Security issues among slices and inside slices need to be addressed by taking into consideration the security coordination and protocols when designing and assigning resources to slices. Therefore, new and advanced security vulnerabilities may be introduced by network slicing deployment in 5G systems and beyond [42].

Each slice is created with isolation constraints set by specific performance indicators to be delivered preventing interferences [43]. With isolation constraints, attack impacts cannot spread over slices and security solutions perform independently. These solutions are required to ensure the common security principles, namely confidentiality, authentication, availability, integrity, and authorization [44]. Confidentiality prevents any disclosure of data to unauthorized users over slices. Authentication verifies the identity of the involved elements interacting with the network. Mutual authentication is required among interacting parties.

Availability ensures the system accessibility and functioning in demand. Defined by the service level agreement, slices and applications need to be reachable when required while NSM and NFs need to be always accessible. Integrity ensures only the slice owners can change, update, or replace the slice functionalities and configuration [45]. Authorization determines the allowed capabilities per network elements. Slice owners are authorized to manage and control their slices, end users are authorized to interact only with allowed slices, infrastructure providers are authorized to control NSM, NSM is allowed to control NSIs and network functions, and network functions are authorized to control resources. These elements include end users, slice owners, service providers, infrastructure providers, NFVs, and NSM. Network slicing security consists of independently fulfilling these requirements by each slice and its owners as the network slicing features can be exploited by attackers causing system failure.

A. Attacks

Network slicing is targeted by a number of attacks disrupting its well-functioning, which may emerge from the isolation level defined by the slice requirements. These attacks may breach one or more of the security requirements. Examples of attacks targeting network slicing include interfaces monitoring, traffic injection, impersonation, denial of service (DoS), tamping, eavesdropping, and reply attacks [41]. Interface monitoring attacks differ according to which interface is targeted, including southbound and northbound interfaces of NSM and the MANO's NFVO [46], [47]. For instance, the NSM interface breach impacts the whole system while the NFVO interface breach impacts only some elements controlled by the NSM.

NSM interfaces monitoring attack occurs when attackers control the traffic over the northbound or the southbound interfaces of the NSM to reveal the system configuration [48]. It aims at capturing snapshots of the system to learn and identify any possible vulnerabilities impacting the confidentiality of

the system. After understanding the system, the attackers can perform other malicious actions breaching the other security requirements. Moreover, attackers can breach the integrity of the system when the northbound interfaces are not correctly validated. Examples of these attacks include traffic injection, impersonation, side channel, and DoS attacks [49].

As data and control planes are not fully separated over the SDN, data plane functionalities interact with the southbound interfaces while control plane functionalities interact with the northbound interface. Side-channel attacks perform across slices sharing resources over common hardware [50]. They can lead to several attacks including hardware tampering, sensor errors, malware, and distributed DoS (DDoS). DDoS attacks occur when malicious users overwhelm a targeted service or a slice by making the network resource unavailable to legitimate users leading to temporarily DoS [51]. These attacks are not easy to mitigate as they perform by flooding the network with traffic making its resources inaccessible for some time, which costs money with high recovery time and impacts negatively the reputation of the victim [49].

Moreover, security attacks can be classified into three main classes: slice life cycle attacks, intra-slices attacks, and inter-slices attacks [52]. Life cycle attacks target the stages of the slice life cycle: preparation, commissioning, operation, and decommissioning. Intra-slices attacks refer to attacks inside a slice while inter-slices attacks refer to attacks among slices. Inter-slice policy refers to shifting management among slices while intra-slice policy refers to slice management itself. Isolation can be used to mitigate the DDoS attacks as slices are running over the same multi-tenant infrastructures, which impacts the slice performance and the resource availability [49].

B. Slice life cycle attacks

A life cycle must be secured as the security vulnerabilities can spread from one stage to the others. Each stage is targeted by numerous vulnerabilities and threats through points of attacks. Preparation stage can be attacked through the network slice template, which is defined at the slice creation. The attacker can exploit a poorly designed template as the point of attacks to launch several attacks including malware and traffic injection. Attacking the template may impact the slices built from it, damage the template integrity, damage the data confidentiality, and change or expose the template content. Examples of the proposed solutions include cryptography and real time analysis. Cryptography based solutions aim at securing the slice template while real time analysis aims at verifying the slice template to ensure it is not tampered in real time [53].

Activation stage can be attacked through APIs, which are used for installing and configuring the slices. The attacker exploits the application programming interface (API) as a point of attacks by either creating fake slices, changing the slice configuration, or missing the slice activation. Examples of the proposed solutions include API security, cryptography, mutual authentication, service request authorization, and real time analysis [54]. API security refers to all the existing techniques for securing an API including access and operational rights. Cryptography based solutions aim at using cryptography protocols for security requirements, transport layer security (TLS) protocols for mutual authentication, and open authorization (O-Auth) for service request authorization [55]. Real time analysis always aims at checking the API and verifying their well-functioning.

Operation stage can be attacked through the slice services and the APIs. Most of the attacks target this stage leading to management problems, configuration modification in run time, and slice deletion. Examples of attacks include DDoS, data exposure, performance degradation, and privacy leaking. Examples of the proposed solutions include slice isolation, security requirements check, and on demand security. Slice isolation aims at addressing the DDoS attacks. Security requirements check aims at avoiding fake instances by ensuring the integrity and the authenticity of the slice [41]. On demand security aims at preventing run time attacks in real time through dynamic NFVs.

Decommissioning stage can be also targeted by several attacks leading to deleted data manipulation and resource consumption. Deleted data manipulation occurs when the used data were not properly destroyed after the slice deletion leading to sensitive data exposure. Resource consumption occurs when the slices are deleted but the allocated resources were not freed leading to DoS attacks. Examples of the proposed solutions include efficient data destruction and resource deallocation. Efficient data destruction allows deleting data definitely with no possible recovery. Resource deallocation allows freeing the busy network in terms of resources and functions.

C. Intra-slice communication attacks

Intra slice security aims at securing a slice network against attacks in the slices [56]. As illustrated in Fig. 3, these attacks can spread inside slices starting from vulnerable points of attacks including user devices, slice service interface, sub-slices, slice manager, resources, and NFs. User device is the most vulnerable point of attacks as it is the front door to slices, services, and network [57]. Examples of attacks targeting the user device include attacks against slices from customers, attacks against customers from slices, and DoS. Slice service interface refers to the interface between the service and the slice and it may be targeted to attack a service itself. Other services running over the slice may be also attacked when the services are communicating directly. Examples of the proposed solutions include proper isolation and service configuration [58]. Proper isolation consists of isolating services between them and isolating services and slices to ensure more isolation over the slice service interface. Service configuration consists of efficiently configure the different services with suitable resources and rights.

For sub-slices, a chain of sub-slices is a point of attacks exploited by the attacker to target the sub-slices and the interconnection between them through the less secure sub-slice [59]. Examples of the proposed solutions include sub-slices security, which consists of ensuring secure interconnection

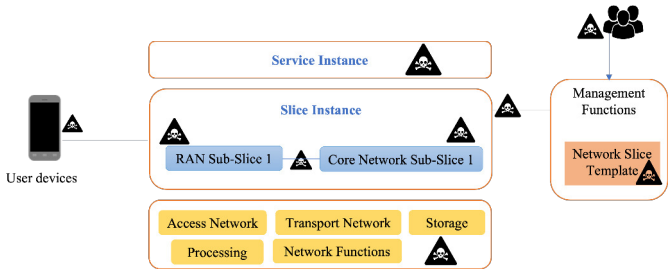

Fig. 3: Intra slice points of attacks.

among sub-slices. For slice manager, it can be a point of attacks as the slice tenants may access unauthorized functions in the legal agreement resulting security managements concerns and multiple points of attacks. Examples of solutions include mutual authentication, which aims at managing the co-existence of several slice managers. For resources and network functions, slices can be attacked through the consumed resources and network functions. Examples of the proposed solutions include mutual authentication, integrity check, secure boot, credential access, and physical security [60].

Intra-slice security includes also the life cycle attacks. They require an E2E security solutions over sub-slices, between slice and slice manager, and between end device and network access point. A number of solutions have been proposed to mitigate with the security attacks in intra-slicing [57]. These solutions are required to respect a number of security recommendations including: each slice is required to get minimal security measures, strong isolation is a must either inter or intra-slices, data isolation is required when a device simultaneously access multiple slices, slices communication should be limited and secure, sharing sensitive parameters and cryptography keys must be forbidden, ensuring security solutions regardless the available resources per slice, sharing resource among slices with different security requirements must be avoided, security mechanisms for each slice including authentication and access control must be independent.

D. Inter-slice communication attacks

Inter-slice security aims at securing a slice network against attacks relying upon other slices. As illustrated in Fig. 4, these attacks can spread across slices starting from vulnerable points of attacks including user devices, service-service interface, RAN sub-slices, management systems, and resource layer. User devices are always at high risk to be attacked when an end user attempts to access an unauthorized slice or to excessively consume shared resources leading to a flooding attack [61]. A user device may be allowed to access one slice or several slices when multiple services are needed, which may lead to other security attacks and security degradation. As these slices are delivered with different security requirements, a user device can leak confidential information from more secure slices to less secure ones. To cope with attacks caused by the customer devices, a full isolation between slices is required limiting users' access and enhancing the security requirements. Examples of isolation techniques include VPN based with SSL/TLS, VLAN based, and tag-based isolation with multi-protocol label switching (MPLS) [62].

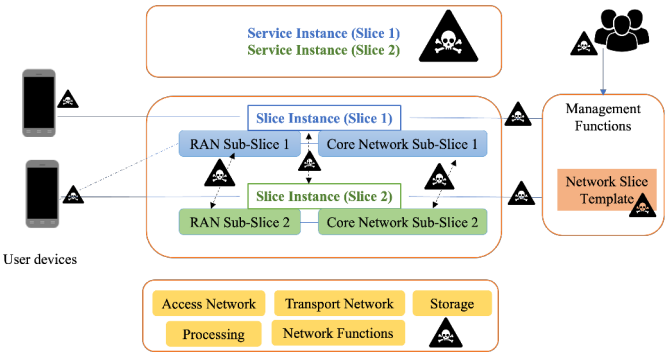

Fig. 4: Inter slice points of attacks.

Resources must be also controlled to avoid DoS attacks by efficiently configuring the resource consumption among slices. Resource capping and ring-fencing are examples of solutions proposed to mitigate the high resource consumption by customers to ensure security requirements [63]. Interface between services using multiple slices is one of the vulnerable point of attacks in a service-to-service communication. When a service is under attack, the attack can spread to other services running over other slices leading to their security damage. Services are usually independent which decreases the risk of the security breach over the different slices. Examples of solutions include isolation, anomaly detection, traffic behavioral analysis, traffic capture, traffic isolation, and artificial intelligence (AI) based techniques. A proper isolation is required to deny any communication among services or slices and cope with attacks between services. Traffic isolation aims at enforcing some security rules by controlling and limiting the traffic flow over the slices.

RAN sub-slice may be attacked as a less secure slice to target more secure slices when the communication among slices is authorized [64]. Consequently, several attacks may occur including parameter leakage, unauthorized access, and sensitive data sharing. Examples of the proposed solutions include isolation, communication security, service communication control, and cryptography based. A proper isolation is required between slices to prevent an attack in a slice from impacting the other slices. A secure communication allows securing and controlling how the slices are interacting and communicating. Service communication control aims at preventing the possible attacks over the service-service interface. Cryptography based solution forbids sharing any cryptography keys between slices to prevent data leakage. Key management can be ensured through the key derivation function to generate new and independent keys for each slice.

Management systems are another point of attacks where an illegitimate tenant can launch malicious activities to modify parameters or access slices owned by other tenants. Examples of the proposed solutions to prevent these attacks include isolation, authentication, and access control. Isolation consists of restricting tenants from making any changes of shared parameters between slices owned by different tenants. A strong authentication is required to enhance the system management

and fight against advanced attacks. Resource layer is also considered as a point of attack as the resource infrastructure is shared and used by all the slices which facilitates the spread of the attacks. Attacking the resource layer leads to resource consumption, DoS, and software attacks. An example of software attacks occurs when an attacker accesses a software used in a slice and tamper its code leading to attack spread to other slices executing the same tamped code [18]. Examples of proposed solutions to prevent these attacks include isolation and code protection. Isolation aims at isolating the code while the code protection aims at protecting it from any illegal access or modification.

E. Comparison

Network slicing attacks are classified according to how and where the attack is launched. These attacks categories are different from one another in terms of attack target, severity, and duration. These differences may be evaluated and compared to determine which security solutions can work for which attacks category. Attacks targeting the life cycle of a slice mainly target the network slice template to damage its integrity and confidentiality. They can access the template content, change the slice configuration, manipulate the data, modify the management parameters in run time, consume resources, or delete the slice. The outcomes from these attacks are severe with major loss. As these attacks can be launched from the slice creation and spread over the other life cycle stages without being detected or mitigated, they may take longer compared to the inter and intra slice communications attacks. Intra-slices attacks mainly target the user device, slice service interface, and slice services.

Services attacks inside the network slices expose the costumers data to illegal access and denial of service. When different services running inside a slice are communicating, service providers and operators can be under potential vulnerabilities as the service based architecture of an operator can be manipulated. Intra-slices attacks can damage only the inside of the network slice; however, sub-slices attacks represent major outcomes as less secure sub-slices may be attacked easily to target other sub-slices. Inter-slices attacks mainly target other slices as the attacks spread over the different network slices. As the same user devices can access several services provided by different slices, the inter slices attacks may target slices with weak security policy to access potential slices with sensitive services. When different network slices can communicate, attacks with high severity may threat the network slicing. Inter-slices and intra slices attacks can take longer as they cannot be detected and mitigated in real time when the attack detection time depends on the services and the application types and cannot be defined in real scenarios. They also include the life cycle attacks leading to attacks with long durations.

IV. Security solutions

A number of solutions have been proposed to address the different security concerns in the network slicing. These security solutions refer to prevention, mitigation, detection, and countermeasures strategies to efficiently protect network slicing systems from any possible threats [65]. They can also be classified into three main categories, namely RAN, core network, and general solutions. RAN's slice solutions consist of mitigating the security attacks targeting the RAN between the end users and the base stations. They aim at protecting the data flow over the RAN. Examples of the proposed solutions include chaos-based cryptography and stream cipher for intra-slice communications [66]. Chaos-based cryptography solution is based on the signal properties to preserve the users and data privacy. Stream cipher-based solution perform by generating a lightweight random number to protect the communications inside the slice.

Core's slice solutions consist of addressing the security issues occurred over the core of the slice network. Examples of the proposed solutions include authentication based, cryptography based, and isolation based. The authentication-based solution allows users to anonymously establish connections with the core network while anonymously accessing the internet of things (IoT) services efficiently [67]. It addresses most of the traditional security threats over the slice network by using the Diffie Hellman key agreement.

Moreover, internet of everything (IoE) technology is also involved in deploying network slicing, which again creates more security issues as everything is interconnected and thus connected to the internet. To protect the security and the privacy of the network slicing in the IoE context, 5G services should be designing as services-oriented authentication.

Cryptography based solution aims at securing the communication between slices. It performs by using public cryptosystems to mutually authenticate at each time a network slicing is accessed [68]. Isolation based solution aims at isolating virtual resources to prevent inter-slices breaches. Most of the proposed solutions focus on the RAN, which cannot be implemented over the packet core and others can only address the traditional attacks. Security attacks can be categorized into two main categories, namely traditional and nontrivial attacks. Traditional attacks are the classical attacks, which have been previously addressed in several services including data integrity, mutual authentication protocols, and encryption strategies. Nontrivial attacks are the open issues which need to be addressed, including avoiding the compromise of a network function, dealing with end-devices vulnerabilities, and defending against side-channels.

When a slice is attacked, it is very important to prevent the spread of the attack to the other slices and impact their security. To protect other running slices over the same network, a number of solutions have been proposed including real time analysis, dedicated security zones, automated security measures, advanced security monitoring, and cross domain security enforcement [69]. These prevention strategies allow isolating the less secure slices from the more secure slices to protect sensitive and critical services.

A. Isolation

Strong isolation is one of the major security solutions to separate parallel slice running on the top of a common network

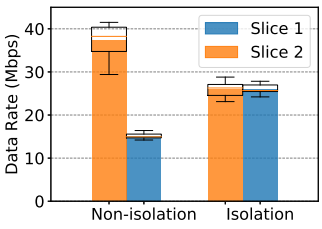

Fig. 5: Performance isolation for Downlink

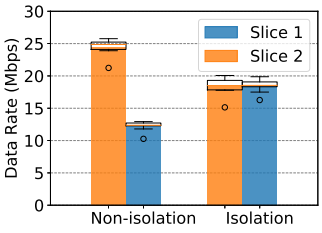

Fig. 6: Performance isolation for Uplink

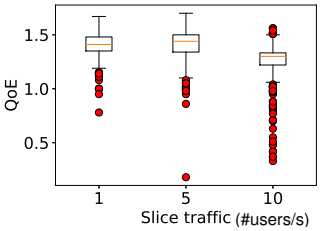

Fig. 7: Anomaly detection with statistical distribution

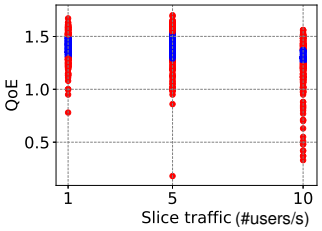

Fig. 8: Anomaly detection with isolation forest

with shared resources [58]. QoS Isolation ensures sharing resource among slices while satisfying the minimum QoS requirement for each slice over dynamic networks. Isolation allows eliminating any direct or indirect relationship or links between slices or other entities involved inside or outside the slice including NFs, end users, network interfaces, and service interfaces. It refers to security, dependability, and performance and can be physical, logical, full, or partial [54]. Physical isolation refers to the separation in terms of physical infrastructure and resources including hardware, firewalls, gateways, and operating systems [70]. However, physical isolation is expensive and often infeasible, which requires introducing the logical isolation for easy and cheaper separation. Logical isolation can be ensured through virtual machines, cloud based, programming codes, trust zones, and hypervisors.

Isolation can be achieved through several requirements including performance, security, privacy, and management. Performance isolation occurs when the required performance by a slice is achieved regardless the performance degradation and the security issues on the other slices. Security and privacy isolation aim at ensuring a specific level of security required by each slice regardless the attacks and breaches occurred in other slices. It requires that each slice has a specific security level ensured via independent functions preventing any unauthorized access to modify the slice configuration or management. Management isolation aims at managing each slice independently by considering it as a separate and isolated network [71]. Isolation level must be enforced among slices at the slice creation, virtualization, and orchestration. To achieve the isolation requirement, a number of approaches have been proposed defining a set of policies and rules to respect by each slice to properly implement isolated slices while maintaining end user services requirements. For instance, slice isolation can be used to mitigate the DDoS attacks in network slicing.

On the other hand, isolation can be an inter-slice isolation or intra-slice isolation. Inter-slice isolation consists of completely isolating the hardware resources to prevent sharing them between slices. It allows protecting the network slices against multiple attacks by preventing the spread of the attack between slices. Intra-slice isolation consists of separating the hardware resources between the involved components inside slices. It provides more security against attacks by decreasing the impact of the attacks with high resource availability and low recovery time.

We show an example of the performance isolation on preventing malicious attacks in Fig. 5 and Fig. 6. We consider there are 2 slices, where slice 1 has two users and slice 2 has one user. We measure both uplink and downlink data rate of slices under non-isolation and isolation RAN. Fig. 5 represents the performance isolation against the data rate for downlink and Fig. 6 represents the performance isolation against the data rate for uplink. Without performance isolation in RAN, the user scheduling and resource allocation (e.g., physical resource blocks) in the MAC layer usually follows the throughput maximization criteria. As a result, the overall data rate of slice 1 is double as compared to slice 2, as all users use *iperf3* to saturate the data rate and RAN treats all users as the same priority. In contrast, with performance isolation, the resources of a slice are exclusively reserved only for this slice's users in RAN. Thus, the achieved throughput of slices becomes almost identical as we assign half resources in RAN for each slice. These results verify the effectiveness of performance isolation on guaranteeing the resource reservation of slices and thus maintaining their performances.

B. Artificial intelligence

Artificial intelligence (AI) technology has been considered to solve some of the security issues in 5G networks and beyond. A number of AI based smart techniques have been proposed to secure the network slicing against severe attacks bypassing basic intrusion detection systems (IDS) and filters. In [72], the authors proposed a deep learning-based framework for secure network slicing in 5G networks. In [73], the authors proposed to consider the involved elements for network slicing security by studying different perspective, namely vertical, horizontal, and multi-lateral. Vertical perspective refers to the involved infrastructure providers and tenants. Horizontal perspective refers to the involved stakeholders in the end-to-end communication. Multilateral perspective refers to security as a service. To treat the security attacks intelligently and effectively, AI based security solutions perform by following the smart slice security cycle: identify, protect, proceed, and recover. Examples of AI based solutions include pattern matching or anomaly detection for attacks detection and identification, source code morphology for protection, and open-source intelligence (OSINT) for awareness [74].

Moreover, the application of new and advanced AI based solutions attracted interest from researchers to enable secure and intelligent network slicing and resource orchestration. Examples of these emerging solutions include federated learning and edge AI [75], [76]. Federated learning based solutions aim at learning how to secure the network slicing via collaborative

learning over a distributed network. Edge AI based solutions aim at performing the intelligent learning at the edge. Security challenges raised from network slicing and its implementation in 5G systems open the door to more strong security issues and customers' privacy. As network slicing performs mainly with NFV and SDN for network virtualization and isolation, these enablers technologies have their own security attacks and issues to be addressed as well [77]. There is increasing popularity of leveraging AI/ML techniques to detect, identify, and resolve various attacks in the area of networking.

Consider a slice hosts an application, where the network operator targets to maintain its performance requirement evaluated by QoE of slice users. We build a first-come-first-out (FIFO) queue in the server to process the incoming requests from mobile users. During the operation of the slice, various attacks might be enforced to compromise the slice performance (e.g., if QoE is less than 1.0). We show several promising techniques to detect anomalies for attacking network slicing in Fig. 7 and Fig. 8. The most common way of detecting outliers is statistical distribution, where the slice QoE is assumed to follow certain prior distributions such as Gaussian distribution. Based on the properties of these distributions, the confidence interval can be calculated, which provides a great standard to determine if the slice QoE is an outlier. In Fig. 7, we used *boxplot* to show the outliers of slice QoE under different slice traffics, based on prior Gaussian distribution. There are more outliers when the slice has 10 active users because the queuing and transmission are more crowded as compared to that of 1 slice user. Besides, we use isolation forest to detect the outlier in Fig. 8, which is another effective way to detect outliers by directly isolating randomly selected features from the whole dataset. As a result, we observe more outliers generated by the isolation forest, as compared to the statistical distribution.

C. End-to-end security

As an end-to-end logical network, network slicing requires an E2E security solution with business model covering all the network domains, namely radio access, transport, and core networks. End-to-end security involves the proper isolation and orchestration [69]. Management and orchestration (MANO) involves three main functions associated with each network slicing layer. It aims at managing the slice life cycle while automating the virtual resource allocation as it is directly connected to the NFV orchestration. From the 5G novel radio multi-service adaptive network (NORMA) project perspectives [30], [78], an SDN based orchestrator (SDN-O) has been proposed to enable inter-slice resource allocation. It requires efficient security strategies to prevent cross slice attacks according to the delivered services capabilities and requirements. Artificial Intelligence integration has been considered to automate the resource orchestration while maintaining some security level. The orchestration security must be adaptive and flexible as the slices are changing with the dynamic services and varying requirements over time.

In addition, E2E security consists of security the E2E network slicing and ensures providing the required security level for different deployment scenarios. With dynamic deployment, E2E security requires an E2E architecture to protect the data from leaking outside of the slices under any conditions or scenarios. Before the network slice is deployed over a shared physical infrastructure, security functions are integrated and SLA contracts are established between the resource provider and the SP and between the vertical service provider and the SP, respectively. The SLA contract defines more details about the network slice including the QoS requirements to deliver a specific service with such performance level.

Blockchain based solutions have been proposed to enable E2E security through smart contracts for various scenarios and services. In [79], the authors proposed a trusted architecture based on Blockchain to secure the network slicing. The proposed architecture guarantees an E2E security by automatically managing only one established SLA between the involved parties. In [80], the authors proposed an E2E trusted architecture based on Blockchain for secure network slicing. This architecture allows ensuring an E2E security and establishing a trusted interconnection through anonymous transactions and SLA management between the concerned actors. It allows managing various SLAs established by involving different actors. In [81], the authors proposed a secure network slicing architecture based on slice brokering, which enables dynamic lease of resources by the infrastructure providers. They secured the network slicing by using decentralized storage platforms to perform the functionalities of a network slice broker. Examples of these platforms include Storj with end to end encryption.

Moreover, E2E security can be ensured by dedicating a slice for securing the network slicing and its different systems [21]. The security slice focuses on detecting and mitigating any security vulnerability over an E2E supply chain. A number of services and functionalities can be implemented over the security slice including incident and event management, monitoring, access control, authentication, and auditing. Network resources are then available and dynamically distributed for security services, which ensures resource availability and E2E security. Security policies are dynamically aligned with the requirements of the network slices and the physical infrastructure.

On the other hand, E2E security can be performed with an E2E isolation of the network slices in such targeted and complex systems. Providing an E2E isolation requires securing and isolating the E2E services themselves with an E2E QoS, which is supported by SLA with the service oriented architecture of the 5G networks [82]. In citewichary2022network, the authors proposed to enable the slice controllers to perform security functionalities at different layers of the network to isolate services and resources in the presence of attacks. They analyzed how to orchestrate and manage resources in a multi-layer architecture under DDoS attack. They defined and selected the classes of key parameters impacting the slice security to consider them while configuring slices and orchestrating resources. These parameters are included in the service level specifications (SLS) for E2E security at high and low levels.

D. Cryptography

Cryptography allows securing and preserving the privacy of a slice through several techniques including Chaos based cryptography, public key infrastructure, and certificateless cryptography. Strong cryptography schemes allow protecting the network slicing from various intrusion by securing the weak links. Existing crypto-systems are not efficient at completely securing the network slicing, which requires replacing them by the quantum-safe cryptographic schemes including post-Quantum cryptography, Quantum key distribution, and symmetric key distribution. In [83], the authors proposed to use signature groups to authenticate or to access even authorized slices of services. Users are required to be identified for any type of communication among slices or exchange messages across slices. They are required to generate new keys for each occurred communication to prevent reply attacks.

In [84], the authors exploited the quantum-resistant algorithms to secure the network slicing through the post-Quantum cryptography and the Quantum key distribution. The proposed solution allows distilling the secret key from the pre-shared key used for authentication and data exchange among slices. In [85], the authors proposed a mutual authentication technique based on symmetric cryptography with secure key distribution to secure the communication. This technique allows sharing the symmetric key among users belonging to the same group of users.

In [86], the authors proposed signcryption schemes for mutual authentication between slices. These schemes enable authenticating slices deployed in different public keys of the infrastructure and the cryptography environment. They enforce the security among slices with digital signature and encryption to ensure confidentiality and integrity. In [17], the authors proposed to use Chaos based cryptography to preserve the privacy over the RAN network and secure the communications among slices. In [87], a cross layer authentication scheme has been proposed for 5G networks by combining cryptographic and non-cryptographic techniques. Moreover, cryptographical solutions have been used to prevent the access to the NST and explore its content for probe purposes and to avoid the leakage among slices [16].

E. Comparison

Various security solutions have been proposed to address the security concerns introduced by the network slicing. They mainly aim at defending the slices against the possible threats while preserving the security requirements. However, deploying these solutions can lead to the performance degradation of the slice services or be a point of attacks for new threats. For instance, isolation is one of the potential solution allowing isolating the slice from any attacks impacting other slices in the same network to spread. It may require exclusive network resources to perform in hard mode with no possible interaction among services. Allocating exclusive resources to a specific slice may impact the other slices needs in resources and quality of service. For soft mode, efficient isolation requires sophisticated methods to share resources among slices. Full isolation offers more security but it degrades the network performance when managing slices independently with high cost.

For artificial intelligence based solutions, they mainly perform by using machine learning and deep learning algorithm to effectively detect and predict attacks in network slicing [88]. They can come up with new threats to the network including logic corruption and data poisoning. The machine learning algorithms allow training models based on some datasets that can be manipulated and poisoned leading to inaccurate results. After a model is maliciously trained with logic corruption, it can be loaded for predicting on new datasets.

For E2E security and cryptography, they provide high level of security but they require the same level of security and cryptography for both end parties with continues updates. Revealing cryptographic protocols for a slice can be exploited by the attacker to ruin the security policies in other slices sharing resources. For time sensitive or critical services, it may be difficult to access the slice services or to authenticate with strong end to end encryption. Other disadvantages refer to the general drawbacks presented when using E2E security and cryptography based solutions with poor designed systems.

V. Discussion

Network slicing security solutions are not yet ready for definitive analysis as the security specifications of the 5G networks are still not standardized yet. Other security risks will appear from the emerging technologies and services, which requires more efforts to develop advanced solutions for the expected and the unexpected vulnerabilities facing either the future networks in general or the network slicing in particular [25]. Therefore, network slicing deployment is facing a number of security challenges impacting several aspects including end-to-end security, performance, resource management, and regulation.

New and potential attacks are raised from different points of attacks over the different layers and network domains. With an end-to-end communication, multi-level security solutions are required to address the security issues over the life cycle of the slices, intra slices, and inter-slices [30]. Isolation cannot be ensured across slices with sliceable RAN when multiple slices share the same access network while demanding distinct physical resource requirements. End-to-end security allows securing the communication from third parties access, but it also can be limited when proper slice isolation cannot be achieved [49].

For performance issues, they occur when implementing network slicing over a common shared infrastructure where a proper isolation requirement cannot completely be ensured. Preserving the performance isolation leads to preventing sharing resources among slices. It may be achieved by assigning dedicated resources per slice, which depletes resources that are finite and expensive. Thus, there is a trade-off between resource sharing and ensuring performance isolation, which can be achieved when preventing resource sharing leading to high resource consumption. Strong isolation requires separating hardware resources and running slices over different physical infrastructures [36]. Therefore, the deployment of the network

slicing solutions requires designing appropriate and efficient resource management strategies for sharing resources while maintaining performance isolation and performance level required by the end user. In addition, resource management and orchestration are challenging the network slicing deployment in a multi-tenant dynamic environment. Given that resources are assigned on demands in function of the time, resource optimization solutions are required to efficiently design resource allocation techniques enabling services delivery with shared resources without violating the required security level.

For the regulation, the network slicing deployment is still under research to define how it will be integrated within the existing infrastructure while achieving the promising performance and business models. Transition to network slicing needs distinctive requirements in terms of compatibility, interoperability, regulation policies, security solutions, cost sharing, billing, and new business models. It involves multiple entities and parties including service providers, operators, tenants, and vendors. Thus, there is a need for standardized security solutions as each involved entity defines its own strategies and policies based on its objectives and priorities.

In addition to these challenges, network slicing security suffers from other issues relative to specific attacks and security implementation. As one of the well-known attacks, DoS attacks are exploited to launch severe attacks on weak slices when the service provider is busy solving the DoS attack problem. They can be mitigated with strong isolation, but slices cannot be completely isolated in resources or network traffic. Some slice information can be exploited by malicious users to identify the slice statute and learn easily how to breach the slice. Examples of these information include slice type, service type, configuration type, slice statute, slice selection, authentication protocols, users request, users connection, and disconnection. Moreover, when a massive number of users need to join a specific slice, they send high number of authentication requests increasing the traffic load leading to attacks from local nodes.

Security solutions involve prevention, protection, detection, mitigation, and countermeasures techniques. Implementing these solutions requires adopting appropriate RAN, which may be solved by using mm-waves for small cells coverage to isolate each cell and implement it with its specific solution. They define how the attack can be detected and which players can recognize the attack including infrastructure providers, operators, service providers, or other tenants. Infrastructure providers and operators cannot detect if a slice is under attack, which is due to the insufficient information they have about the traffic loads legitimacy and the resource usage by the service providers. Service providers cannot detect the attacks as they cannot correctly interpret the changes in the network as malicious activities [89].

In order to address these security challenges facing the network slicing deployment, several future directions can be considered including artificial intelligence and Blockchain based solutions for strong isolation and resource management. Resource sharing is one of the key issues leading to security vulnerabilities among slices. Resources are shared between different tenants through static or dynamic partitions. Dynamic resource partition allows efficient network sharing, but it requires strong management and scheduling strategies with high isolation, less computational cost, and low response time. Operators are required to respond rapidly to customers' requests to create and manage slices over a dynamic service load.

In addition, RAN slicing can be enabled through identifying each sub-slice with unique identifier to enforce different level of isolation while maintaining required performance. Moreover, slice management configures slices with specific security requirements. When some slices sharing resources with other slices need permissions to perform some actions, security in the other slices may be impacted due to configuration errors or inter attacks requiring automated management. Thus, there is a great need for efficient and intelligent strategies able to assign unique identifiers to the massive number of slices and sub-slices with no errors [36]. For isolation, there is no full isolation among slices in real scenarios as control plane and data plane are not completely separated. Some critical services require shared control functions inter-slices, which spreads the attacks among slices. Real time services are vulnerable to interferences and require fast handover for better QoS, which impacts the slice security. Slices are created to deliver services in the cloud with virtual resources [42]. Therefore, designing effective and smart strategies is required to ensure strong isolation in both virtual and dynamic environments. Therefore, artificial intelligence is expected to solve any of today's issues, which can be also considered for resource management in multi-tenant and dynamic context. Deploying network slicing based artificial intelligence can ensure predicting how many resources are needed to perform a service no more no less, detecting, and preventing security vulnerabilities before they are even launched. New business models are required to regulate the resource sharing among multiple providers [36], [90].

As the network slicing involves multiple entities with distinctive roles from infrastructure providers to end users, Blockchain is one of the promising solutions to be investigated for further research. It allows determining how the billing will be performed by each entity and how the infrastructure providers can distribute and allocate their resources to different tenants. Infrastructure providers may need to involve other intermediate players to interconnect with different tenants to distribute and share resources among slices while maintaining a certain level of security, flexibility, and scalability.

VI. Conclusion

In this paper, we have presented an analysis of the security challenges facing the network slicing and how to address them through a number of solutions. These security challenges open the door for severe and multi-faced security attacks impacting the service providers, operators, tenants, and end users. Isolation and artificial intelligence based strategies can be considered in order to mitigate the security issues and to protect the network slices from third party attacks. We have implemented these solutions and evaluated their performance. Through analyzing the simulation results, isolation and ma-