




Review

Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey

Shujuan Gao, Ruyan Lin, Yulong Fu ^{*}, Hui Li  and Jin Cao 

School of Cyber Engineering, Xidian University, Xi'an 710126, China; gsj@stu.xidian.edu.cn (S.G.); ruyanlin@stu.xidian.edu.cn (R.L.); lihui@mail.xidian.edu.cn (H.L.); jcao@xidian.edu.cn (J.C.)

* Correspondence: ylfu@xidian.edu.cn

Abstract: Network slicing empowers 5G with enhanced network performance and efficiency, cost saving, and better QoS and customer satisfaction, and expands the commercial application scenarios of 5G networks. However, the introduction of new techniques usually raises new security threats. Most of the existing works on 5G security only focus on 5G itself and do not analyze 5G network slicing security in detail. We consider network slices as a virtual logical network that can unite the subnetwork parts of 5G. If a 5G network slice has security problems or has been attacked, the entire 5G network will have security risks. In this paper, after synthesizing the existing literature, we analyze the security threats step by step through the lifecycle of 5G network slices, analyzing and summarizing more than 70 security threats in three major categories. Based on the security issues investigated, from a viewpoint of building a secure 5G network slicing system, we compiled 24 security requirements and proposed the corresponding recommendations for different scenarios of 5G network slicing. Finally, we collated the future research trends of 5G network slicing security.

Keywords: 5G mobile internet; network security; network slicing; SDN/NFV security; network resource isolation



Citation: Gao, S.; Lin, R.; Fu, Y.; Li, H.; Cao, J. Security Threats, Requirements and Recommendations on Creating 5G Network Slicing System: A Survey. *Electronics* **2024**, *13*, 1860. <https://doi.org/10.3390/electronics13101860>

Academic Editors: Lei Shu and Andreas Mauthe

Received: 14 April 2024

Revised: 2 May 2024

Accepted: 8 May 2024

Published: 10 May 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The 96th meeting of 3GPP RAN announced the freezing of 3GPP R17, marking the official completion of the second evolutionary version of the 5G standard. Compared to traditional wireless networks, 5G mobile networks innovatively adopt technologies like software-defined networking (SDN), network function virtualization (NFV) and network slicing. These technologies are used to ambitiously meet today's higher wireless communication demands, which include speed, low latency and enhanced capacity.

Network slicing [1] is a revolutionary concept for enabling mobile networks on demand. The essence of 5G network slicing is to run multiple virtual logical networks [2] on a common physical infrastructure in an efficient and economical way. The independence and freedom to divide resources on demand allow 5G network slicing to adapt to social scenarios with complex environmental conditions.

With network slicing, many special network scenarios can be supported. For example, in medical-related scenarios, the low latency, large bandwidth and flexible combination of 5G slices can better respond to unexpected situations during patient treatment. With 5G network slicing, "online consultation" is no longer empty talk. In the urban construction scenario, 5G network slicing provides new ideas for smart city implementation. The combination of multiple types and large numbers of 5G slices can be used to guarantee many smart city operations, such as geographical conditions, economic base and population size, etc.

Traditional telecommunication operators are generally considered secure due to their robust network infrastructures. They employ various security measures, including firewalls, intrusion detection systems and VPN connections. These technologies help to isolate

their networks from potential attackers, enhancing overall security. However, the emergence of network slicing involves the creation of multiple virtual networks on top of the 5G physical infrastructure and shared network resources, which may introduce new potential vulnerabilities and increase the attack surface; there will be security threats in 5G networks that traditional security solutions cannot cope with. Chen, Y. Z. et al. [3] highlight that shared network resources can lead to various security vulnerabilities, such as cross-slice attacks and resource hijacking. These studies indicate that attackers could exploit improper configurations or vulnerabilities in shared resources to conduct cross-boundary attacks, affecting multiple users and services. Therefore, in order to ensure the secure deployment and implementation of 5G network slicing, it is urgent and necessary to build a holistic security framework that contains security threats, security requirements and security recommendations.

2. Related Work

Recently, the security issues of 5G network slicing have attracted widespread research interest in academia and industry. Khan et al. [4] analyzed the underutilization or overutilization of resources due to unreasonable division of fixed resources within network slice security concerns and pointed out the need to design resilient network slices. Wong et al. [2] focused on the security isolation problem for multi-tenant scenarios with multi-network slicing deployment. However, to a certain extent, the existed work focuses only on the security of slicing inside 5G networks and some slicing security issues caused by external factors are ignored. Dangi et al. [5] introduced the security threats faced by slicing in terms of slicing lifecycle (preparation, instantiation, operation and retirement), focusing on investigating the application of machine learning in solving slicing security problems. However, the focus of the authors' research is concentrated on the application of machine learning in slicing security solutions, ignoring the exposure of slicing security threats. Olimid et al. [6] investigated the slice lifecycle security, intra-slice security and inter-slice security perspectives, and discusses some challenges and unresolved issues of network slice security. Although the authors focus on the security of each phase of 5G network slicing, the summary of related security threats was still not comprehensive.

In the current industry scenario, the development of 5G network slicing technology is rapidly advancing to meet diverse service demands and enhance network flexibility (see Table 1). According to the latest 3GPP standards, the importance of slicing security is increasingly emphasized, necessitating further enhancement of security measures such as slicing isolation, identity verification and data protection. These security requirements guide the ongoing optimization and innovation of the 5G security architecture in the industry.

In this paper, after an in-depth analysis of a large amount of literature related to 5G and 5G network slicing security, we provide a comprehensive summary of the security issues faced in creating a 5G network slicing system, which specifies the security threats, requirements and recommendations through the 5G network slicing lifecycle. We analyzed the security challenges of a 5G network slicing system in three phases. Firstly, before a user requests network slicing, the complexity of security management within the operator's network increases. This is due to the need to deploy a sliced virtual logical network, which requires enhanced data security measures within the network. Secondly, when the slicing network environment is fully prepared, the network needs to securely perform a series of slicing activation operations when receiving a slicing request from users, i.e., data security during user demand analysis and interface security when the demand configuration is issued, etc. Finally, some security issues specific to the sliced network will come to the fore after the slices are put into use, such as authentication security in multi-slice/multi-user scenarios, slicing isolation and sliced network capacity exposure security, etc. The main contributions of this paper are as follows:

- Analyzed and summarized more than 70 security threats from 5G network slicing lifecycle;

- Compiled 24 security requirements for building a secure 5G network slicing system and building a holistic security framework that contains security threats, security requirements and security recommendations;
- Suggested importance classification of security requirements for different scenarios of 5G network slicing.

The rest of the article is structured as follows: Section 3 briefly describes the background knowledge of 5G networks and introduces the key concepts, architecture and management model of 5G network slicing. Section 4 analyzes the security issues in the three phases of 5G network slicing: deployment and activation, as well as operation and maintenance. The security threats faced by 5G core networks are defined. Section 5 organizes the security requirements under different scenarios of 5G network slicing based on the security issues investigated. Section 6 organizes the combination of current popular research directions with 5G slice security and gives an outlook on future research directions. And, finally, we conclude paper in Section 7.

Table 1. Summary of previous studies.

Papers	Year	Contribution in Security Aspects	Note
5G Network Slicing: A Security Overview [6]	2020	The paper highlights threats and recommendations from the aspects of lifecycle security, intra-slice security and inter-slice security. It also identifies and discusses open security issues related to network slicing.	Safety recommendations are not comprehensive enough.
A canvass of 5G network slicing: Architecture and security concern [7]	2020	The authors examined slice lifecycle, inter-slice and intra-slice security threats.	Several threats and vulnerable areas exist that are not covered.
ML-based 5G network slicing security: A comprehensive survey [5]	2022	The paper introduces ML-based network slicing, including threats and attacks during the slicing lifecycle.	Deeper exploration is needed in multiple vulnerable areas.
Towards secure and intelligent network slicing for 5G networks [8]	2022	The paper classifies different attacks targeting network slicing into three main classes: inter-slice, intra-slice, and lifecycle attacks. The paper analyzes how these attacks can be mitigated and evaluated the performance of some of them using Open Air Interface.	Attacks and threats related to other vulnerable areas need to be discussed.
End-to-End Network Slicing Security Across Standards Organizations [9]	2023	The paper analyzes the underlying security threats of network slicing, derives corresponding security requirements and studies specific network slicing protection mechanisms.	Several threats and vulnerable areas exist that are not covered.
Security in 5G Network Slices: Concerns and Opportunities [10]	2024	The core objective of this work is to understand network slices and their potential vulnerabilities, examine the essential security prerequisites and suggest strategies.	Safety recommendations are not comprehensive enough.

3. Background of 5G Network Slicing

5G is the current generation of broadband mobile communication technology with high speed, low latency and high connectivity. It was originally created to meet the social development aspiration of “Internet of Everything”.

The application of a series of key technologies enables 5G networks to meet user service requests in more complex, diverse and demanding scenarios. Among them, “network slicing” makes it possible for 5G networks to build end-to-end logical networks. As security researchers, we should not analyze network slicing as a one-sided application of technical means. We should look at the essence through the phenomenon and focus on the essence of realizing and supporting the safe operation of slicing. This section provides an overview of the background knowledge of 5G network slicing and lays the foundation for the subsequent study of analyzing security threats in the 5G network slicing system.

3.1. 5G Network Slicing Original Idea and Composition

The combination of 5G and network slicing is a bold attempt by researchers to achieve the separation of different types of user traffic and to create a dedicated self-organizing core network. Rost et al. [11] considered network slicing as an effective solution to cope with the various demands of 5G mobile networks, providing the flexibility and scalability necessary for future network implementations. The core idea is that Network Slice Instances (NSIs) deploy logical networks that meet specific service requirements by custom setting network attributes on a shared physical network [12–15]. From the network operator’s perspective, network slicing is a separate end-to-end logical network that negotiates the quality of service of the network but the technology supporting network slicing is transparent to the service customer [16]. With network slicing, service providers can flexibly and easily deliver their services to meet a variety of unique needs, such as virtual and augmented reality, video games and e-health [7].

An NSI can span multiple parts of the network (e.g., terminals, access network, transport network and core network) [6]. The 5G mobile network can be subdivided by function into: radio access network, transport network and core network. The corresponding NSI also consists of a combination of three parts of a Network Slice Subnet Instance (NSSI) [12], namely: RAN-NSSI, TN-NSSI and CN-NSSI. Each part of the NSSI is combined according to user requirements and the combination ratio is not limited to 1:1:1. One or more NSSIs linked together can form an NSI with service functions [6], i.e., an end-to-end 5G network slice is a sub-slice chain formed by network slices from the access network and the core network through the connection of the transport network.

For example, in eMBB and uRLLC scenarios, slices usually share AMF or core network sub-slices composed of AMF and UDM to achieve reduced signaling consumption from access and mobility management, i.e., NSI-B and NSI-C in Figure 1. In addition, in some industrial service scenarios with high sensitivity to data thresholds, such as metal smelting and chemical material production, it is required that 5G core network data control plane with certain reaction arithmetic and the ability to monitor data confidentiality and integrity. At this time, it requires network slicing exclusive core network sub-slices, i.e., NSI-A, NSI-D and NSI-E in Figure 1.

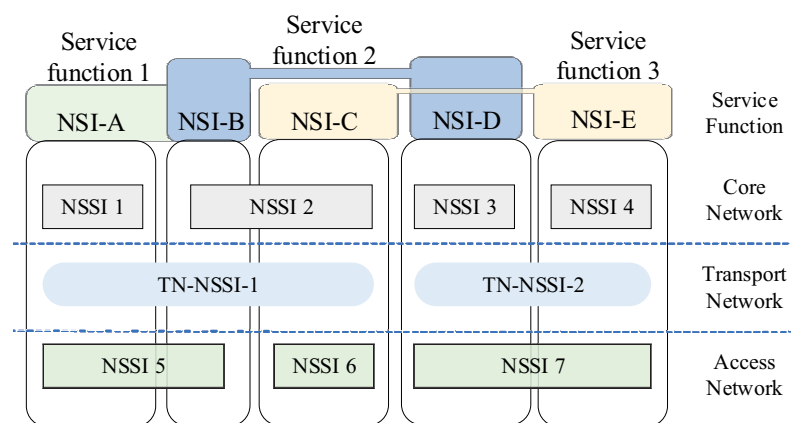


Figure 1. Multi-domain NSSI constitutes NSI to provide different service functions.

3.2. 5G Network Slicing Lifecycle

Network slices, as logical networks that fulfill the needs of communication services, have a lifecycle independent of the communication service lifecycle [12]. Meanwhile, the lifecycle security management of network slices occupies a large proportion of 5G network security requirements. The network slice lifecycle specified by 3GPP TR 23.799 [17] typically includes: Preparation, Instantiation, Configuration and Activation, Run-time and Decommissioning (see Figure 2).

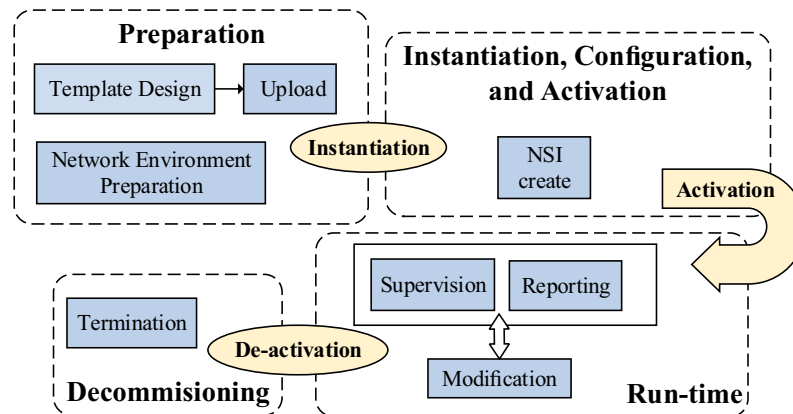


Figure 2. 5G network slice lifecycle.

- **Preparation:** The main work in this phase includes: slice template design and upload, network environment preparation, etc. A slice template, which can be also called a network service template, is essentially a text file describing the user's service requirements. The content of the slice template includes information on the type, number and specification of network elements required for the service, resources and connections, etc. The main work of the slice preparation phase is to complete the invocation of network resources and ensure the allocation of slicing resources at a later stage.
- **Instantiation, Configuration and Activation:** The main work in this phase is to create slices according to the slicing template in the first phase, and complete the resource division, function configuration and service activation of the slices.
- **Run-time:** After the slices are created and put into operation, their operation status needs to be monitored in real time. The main task of the third phase is to monitor the operation status of the network slices and report on the operation data of the slices. In addition, it updates, adjusts and configures the current network slices in real time when the tenant's business requirements change. At the same time, it also has a certain monitoring role for slice failure.
- **Decommissioning:** The slice needs to be logged out after completing its service mission, which is essentially releasing the slice resources and network functions, and the original slice no longer exists after logging out.

Based on the above network slicing lifecycle process, we extracted the key operations of each part and proposed a slicing lifecycle process that is more in line with the actual deployment scenarios, i.e., deployment phase and generation phase, as well as operation and maintenance phases (see Figure 3). Among them, the deployment phase is mainly concerned with the operator's preparations before slice generation, such as network function realization, network architecture deployment and so on. The generation phase is a synthesis of the original Preparation and Instantiation phases; the operation and maintenance phase is a synthesis of the Run-time and Decommissioning phases (see Figure 3).

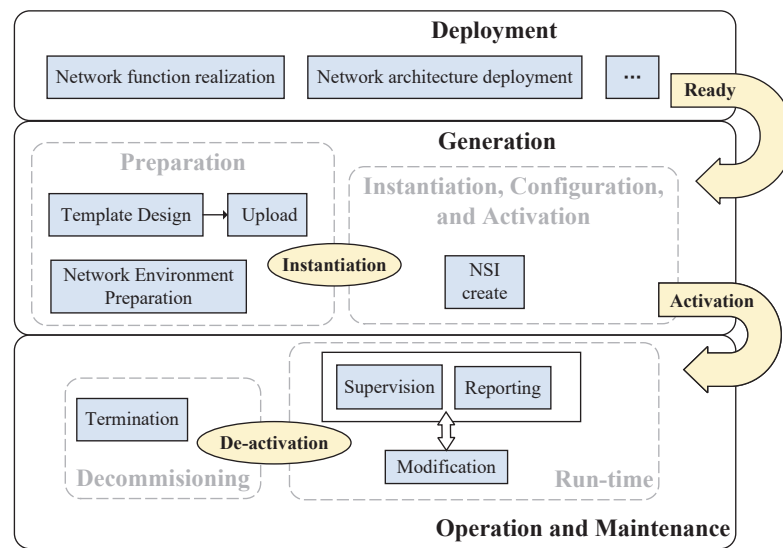


Figure 3. New 5G network slice lifecycle.

3.3. 5G Network Slicing Management and Orchestration

3.3.1. 5G Network Slicing Management Architecture

The management architecture of 5G network slicing runs through the radio access network, transport network and core network as shown in Figure 4, which cooperates with the following main functional components [18]:

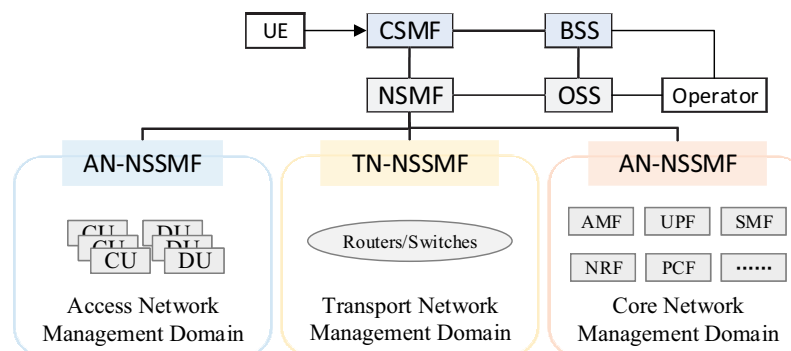


Figure 4. 5G network slicing management architecture.

- BSS (Business Support System): This refers to a class of software programs that help telecommunication operators manage and streamline all customer-facing business activities, such as subscription services, billing issues and subscription upgrades. Because such systems are directly related to the customer business experience, the BSS is critical to the successful operation of modern telecommunications organizations.
- OSS (Operation Support System): This consists of the actual network infrastructure and software used to control the network, and is designed to help telecommunication operators monitor, analyze and manage wireless networks, and to support operators in remotely managing and monitoring daily operations throughout the network.
- CSMF (Communication Service Management Function): This manages communication services, each of which is completed by one or more network slices; CSMF interfaces with the BSS of the operator’s network and is responsible for slicing service operations; slicing users order slices from the operator through CSMF and submit relevant SLA requirements (e.g., number of online users, average user rate, latency requirements, etc.), and the CSMF converts the subscriber’s communication service requirements into network slice requirements for the NSMF and forwards them to the NSMF [19].

- NSMF (Network Slice Management Function): The purpose of the NSMF is managing network slices; each network slice can be composed of several network slice subnets. The NSMF receives network slice deployment requests from the CSMF, decomposes end-to-end SLA requirements of network slices into SLA requirements of network sub-slices and sends network sub-slice deployment requests to NSSMF.
- NSSMF (Network Slice Subnet Management Function): The purpose of the NSSMF is managing network slice subnets; each network slice subnet can be composed of one or more basic sub-slices, where each sub-slice can contain several network functions. The NSSMF is responsible for the orchestration, deployment and maintenance of sub-slices, and different areas of the NSSMF convert the SLA requirements received from the NSMF uniformly for the network slice subnetwork into network element service parameters and issues them to the network elements.

In summary, the CSMF and NSMF are the key entities to realize network slicing management, and the management focus of each of them is different. Among them, the CSMF is responsible for completing the management of slicing services by communicating and interfacing with users. It includes slice order management, customer management, slice service query, etc. As for the NSMF, its management focus is on the details of network slicing.

3.3.2. Network Slicing Management and Orchestration Architecture Based on SDN and NFV

NFV and SDN are the key supporting technologies for 5G network slicing, which make the deployment of many 5G network slices on shared physical devices become possible. In fact, NFV is a concept of network architecture, which emphasizes the utilization of software to apply standardized network functions to a unified standard of hardware [20]. ETSI (European Telecommunications Standards Institute) proposed an NFV architecture (see Figure 5). The framework defines three recognized components: Virtual Network Functions (VNF), Network Functions Virtualization Infrastructure (NFVI) and Management And Network Orchestration (MANO). The components and functions are described below:

- VNF: This is composed of a variety of applications deployed on virtual resources to implement traditional network functions. Different VNFs are usually developed by mutually independent software developers, but those diverse VNFs should adapt to a standardized and unified NFVI architecture.
- NFVI: This provides the hardware and software architecture of the required environment for the deployment, management and operation of NFV. The NFVI includes hardware resources, a virtualization layer and virtualization resources.
 - Hardware resources include computing resources, storage resources and network resources, which provide computational processing power, storage capacity and network connectivity to the VNFs through the virtualization layer (e.g., VMs, virtual machine managers, etc.).
 - The virtualization layer is responsible for abstracting hardware resources into virtual resources using virtualization methods (e.g., Docker, Hypervisor, etc.).
 - Virtualized resources include virtual computing resources, virtual storage resources and virtual network resources. These virtual resources maximize the use of limited hardware resources and are the basis for generating VNFs [20].
- MANO: This refers to a functional framework that manages the lifecycle of VNFs and orchestrates their deployment and operation. MANO is responsible for tasks such as VNF onboarding, configuration, scaling and healing. The MANO framework consists of the following three main components:
 - VIM (Virtualization Infrastructure Manager) is mainly responsible for the lifecycle management and allocation scheduling of hardware/virtual resources in the NFVI, such as the allocation of CPU resources and network link bandwidth.
 - VNFM (Virtualized Network Function Manager) is mainly responsible for VNF lifecycle management, i.e., VNF creation, update, extension and deactivation.

- NFVO (NFV Orchestrator) is mainly responsible for coordinating the management of VNFM and VIM. It makes the creation of the VNF more reasonable and safe, and the operation more reliable and effective [20]. In addition, the NFVO connects to other data repositories, such as the network service catalog, VNF catalog, instance catalog and NFV infrastructure resource database, which contain relevant information about their respective entities. Finally, a series of standard interfaces are set up in MANO to enable communication between different components in MANO and coordination between MANO and traditional network management systems (e.g., OSS, BSS and EMS: Element Management System).

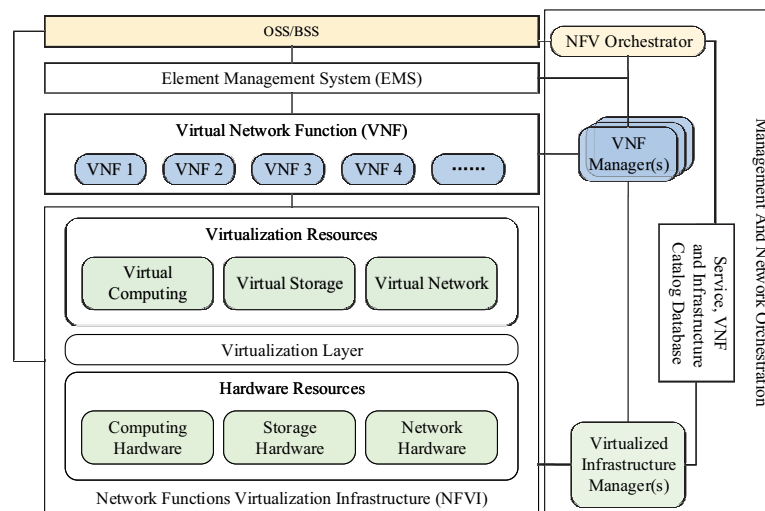


Figure 5. ETSI-NFV architecture.

In order to support the real-time effectiveness of the NFV infrastructure and architecture, the network devices which host NFV must be updated continuously for configuration [21]. However, changes and configurations for traditional network operations are conducted in a (semi-)manual manner over relatively long time periods (e.g., minutes, hours or even days). This makes it difficult for this approach to guarantee the proper operation of NFV-based network slicing solutions. For this reason, it is significant to introduce SDN to help 5G network slicing to achieve dynamic traffic steering and management as well as real-time and rapid establishment of end-to-end network slices. It also fits the needs of the scalability, flexibility, agility and programmability of 5G mobile networks.

SDN is a network architecture that decouples the control plane and data plane as shown in Figure 6. The core idea is to move the control function from the network device to the central device (cluster), so that the control plane and the forwarding data plane are separated. The control engine that was originally scattered on each network device is replaced by the controller centrally. A typical SDN architecture is divided into three layers: the application layer, the control layer and the physical infrastructure layer (data layer). There is an Application Program Interface (API) between each layer, with the northbound API used to control application communications and the southbound API used to control the infrastructure. Among them, the core component that supports the SDN architecture to achieve on-demand provisioning of network resources and flexible service customization is generally the SDN controller. The controller interacts with the upper layer applications and lower layer forwarding devices through the northbound and southbound interface protocols, respectively. It enables top-level SDN applications to programmatically control the underlying hardware through the software platform in the controller.

It is worth noting that the study of SDN Orchestrator (SDNO) deployment has also received much attention in order to realize service collaboration and resource scheduling across SDN domains in multiple scenarios. Usually SDNOs provide unified and automated network connectivity orchestration, service model management, resource management and

performance monitoring control for SDN domains across regions, layers and manufacturers. This helps to improve the openness of network capabilities and the end-to-end automation of services. In turn, it enables automatic network deployment and agile operation, bringing better user experience to customers.

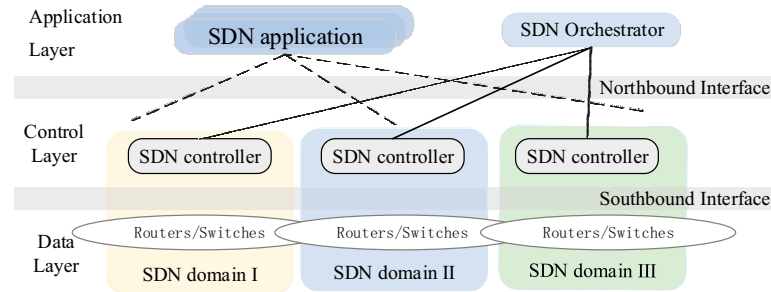


Figure 6. SDN architecture.

SDN technology can provide end-to-end differentiated traffic control, while NFV technology can achieve flexible deployment of 5G network elements in the entire 5G network. This also proves that the technical characteristics of NFV and SDN can well meet the hierarchical orchestration requirements of 5G end-to-end network slicing, thus triggering a research boom in network slicing architecture based on NFV and SDN. Based on the NFV and SDN slicing architecture and the existing slicing management and orchestration framework, in order to comprehensively study slicing security, we summarize a slicing management and orchestration architecture in Figure 7 based on NFV and SDN that can be used throughout the end-to-end network slicing lifecycle by studying the slicing architecture based on NFV and SDN [22] and existing slicing management and orchestration frameworks.

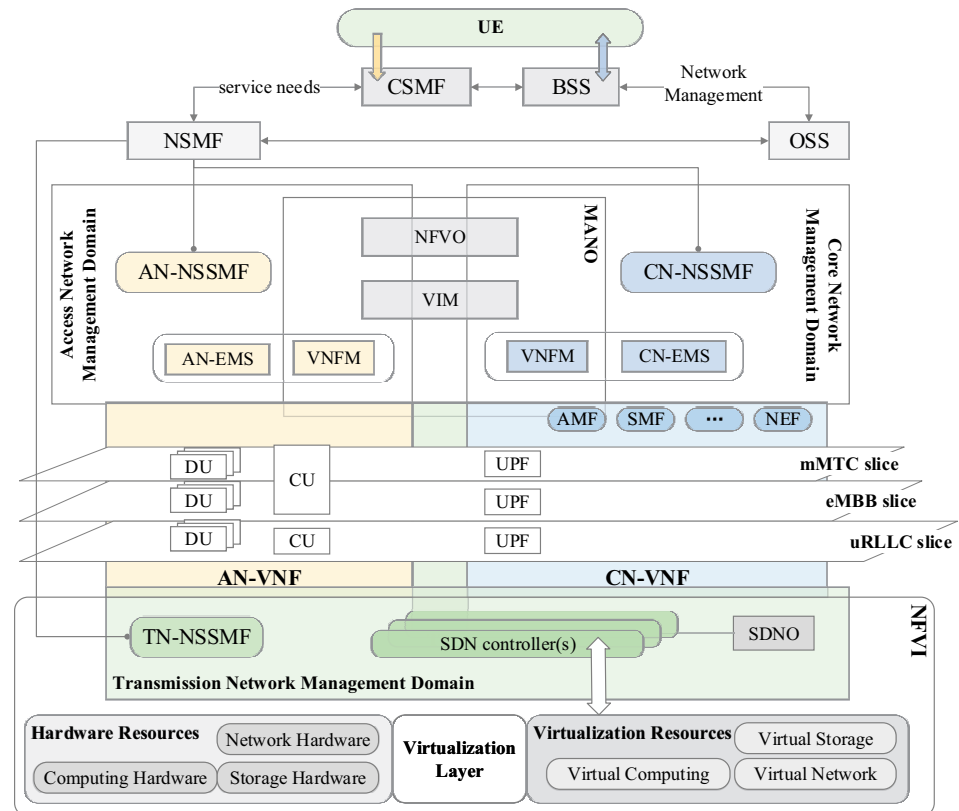


Figure 7. NFV- and SDN-based slice management and orchestration architecture.

In this framework, NFV focuses on how to virtualize existing hardware resources and how to orchestrate the lifecycle management of VNFs. SDN focuses on how to carry and control data plane traffic.

4. 5G Network Slicing Security Threats

Network slicing brings us many advantages, such as empowering operators to offer differentiated services, optimizing resource utilization and improving service quality; however, its virtualization nature also blurs the traditional security boundaries and leads to a series of security issues, such as VM Hopping [23], Vulnerabilities of VMM and Failure to VM Isolation [24]. In this section we are focusing on the security issues of 5G network slices and analyze its security threats within three phases of the 5G network slicing lifecycle, namely, **Slicing Deployment, Slicing Activation, Slicing Operation and Maintenance**. We summarize more than 70 security threats from the three different slice lifecycle stages (see Table 2).

Table 2. 5G network slice security threat.

5G NS Lifecycle	Threat Scenarios/Attack Surfaces	Threats/Attacks/Vulnerabilities	Source	
Deployment	NE registration	1. NE registration template data leakage 2. Malicious NE forgeries and registrations	[25] \	
	NE subscription and discovery	3. Replay attacks on the NRF 4. Hijacking attacks TCP session between NE and NRF 5. DoS attacks on the NRF	[26] [26] [26]	
	NE logout	6. NE decommissioned data leakage 7. Illegal NE registration requests lead to DoS Attacks	[6] \	
	UPF sinking deployment	8. DoS Attacks on the UPF 9. UPF configuration tampering	\ \	
	CU and DU deployment	10. Data leakage and tampering 11. Hijack CU	\ \	
Generation	User request transmission	12. Malicious tampering with user requirements	\	
	CSMF analyzes user requirements	13. Hijack CSMF permission before user's requirements arrive 14. DoS attacks on CSMF 15. Interference as CSMF analyzes user requirements	\ \ \	
	Slice template management	16. Slice template data leakage 17. Slice template data tampering 18. Malicious slice template replay attacks	[7] \ \	
	Public interfaces (PIs)		19. Attack PIs to gain slice management module permissions 20. Attack PIs to gain ComServ Management Module permissions	\ \
			21. Attack PIs to interfere with network slice lifecycle 22. Attack PIs to interfere with communication services configuration	[18] [18]
			23. Replay legitimate messages on public interfaces	\
			24. Destroy the packet before it reaches PIs	\

Table 2. Cont.

5G NS Lifecycle	Threat Scenarios/Attack Surfaces	Threats/Attacks/Vulnerabilities	Source
Operation and Maintenance	Slice selection information	25. Slice service data (related to NSSAI) leakage	[27]
		26. Man-in-the-middle attacks at the connection establishment stage	[27]
		27. Man-in-the-middle attacks on critical services related to NSSAI	\
		28. Data tampering attack against the rejected NSSAI	[27]
	Slice operation monitoring report	29. Tamper with slice report causes incorrect management operations	\
		30. Collect slice reports to fake malicious slices	\
	Slice decommissioning information	31. Slice decommissioning sensitive data leakage	[14]
		32. Slice resources released illegally	[18]
		33. Slice resources released incompletely	[18]
	Opened interfaces of NEF	34. Communication data leakage	\
		35. Unauthorized access	\
		36. Packet hostage	\
		37. DoS attacks	\
		38. Shared data tampering	\
	Opened interfaces of cloud-native 5G	39. Exploiting vulnerabilities or backdoors to illegally access resources	[28]
		40. Manipulating or modifying interfaces to disrupt network slices	[29]
	Cloud-native 5G architecture	41. Misconfiguration vulnerabilities	[24]
		42. Application vulnerabilities	[24]
		43. Malware injection attacks	[24]
	Terminal access slicing scenario	44. Impersonate a legitimate user to access slices	\
45. Data leakage due to access to malicious slices		\	
46. Logical vulnerability in the 5G-AKA protocol specification		[30]	
47. Attack on user location privacy		[31]	
Multi-tenant one-slice scenario	48. User privacy data leakage	\	
	49. Maliciously tampering with shared slice parameters	\	
Multi-slice scenarios with single tenant	50. Low-flow attacks	\	
	51. Attack delivery between slices	\	
Multi-slice scenarios with multiple tenants	52. Attack against weakly secured sub-slices	[6]	
	53. Attack delivery between sub-slices	[14,32]	
	54. Leakage of sensitive data across slice security domains	[33]	
Multi-slice scenarios	55. Attack on shared communication links between slices	[34]	
	56. Attack slice function by using inter-slice communication links	[33]	
	57. Unauthorized access between multiple slice managers	[35]	
	58. Data leakage in multi-slice communication	[36]	
AMF redirection	59. Slice data obfuscation caused by AMF key non-separation	[37]	
	60. Slice data leakage caused by AMF key non-separation	[37]	
5G network terminal users	61. Operators' solutions cannot fulfill all hardware sec. requirements	\	
	62. Improper slice operation by the user	[38]	
	63. Insecure slice usage scenarios	\	
	64. Hijacking of terminal devices	[32]	
5G network physical layer	65. Destruction of physical resources using malware implants	[39]	
	66. Destruction of physical resources using physical attacks	[39]	
	67. Destruction of physical resources using resource consumption	[39]	
	68. Exploit a vulnerability in hypervisor to gain root privileges	[28]	
	69. Basic input/output system (BIOS) attack	[40]	
	70. Side-channel attack (SCA)	[32,39]	

4.1. Security Issues in Slice Deployment

The work related to the deployment of slicing should be ready or in progress before the “operator’s network slicing requirement” is landed. One of the innovations of 5G network slicing is the flexibility to change the “location” of the deployment of network functions but the flexibility deployment of NE (network element) may also lead to many security issues.

4.1.1. Threats on NE Deployment of 5GC

Two virtual network element architectures are proposed in 3GPP for deploying inter-NE communication, namely Service-Based Architecture (SBA) and Reference Point Architecture (RPA). In this subsection we focus on the NE deployment based on SBA implementation. The 5G-CN designed based on SBA principles [41] has a more fine-grained and decoupled network function, and the core network can be internally automated with operational processes to achieve system integration while enhancing operational efficiency [25]. The framework uses NFV technology to provide flexible resource allocation, but also exposes the framework to security threats such as DoS attacks, man-in-the-middle attacks, side-channel attacks, hypervisor hijacking and infrastructure attacks. We will analyze the security of the SBA framework in terms of one NE autonomous operation flow as shown in Figure 8, i.e., registration, subscription and discovery, and logout.

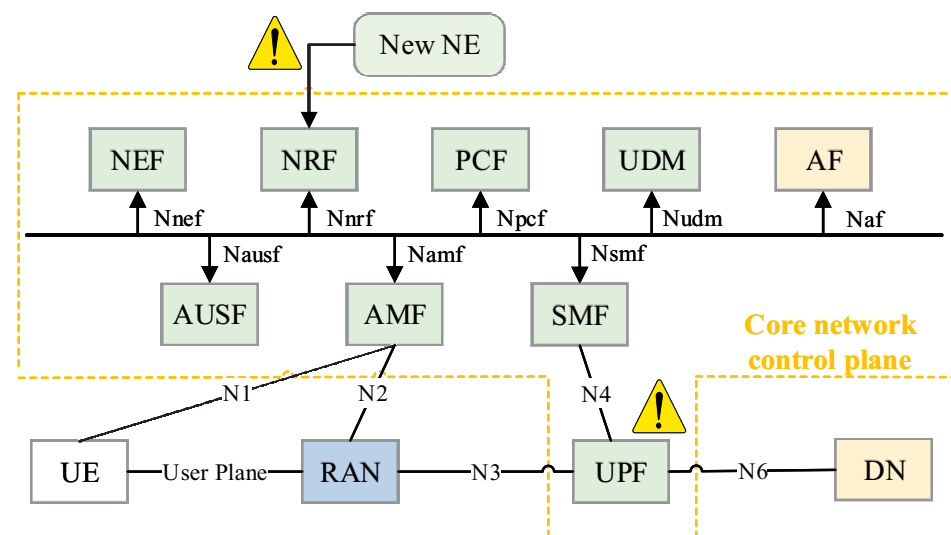


Figure 8. Service-Based Architecture.

1. Security Threats in NE Registration

3GPP briefly defined an NE registration process in TS 23.502 (see Figure 8). When a new NE wants to join the networks, it needs to initiate the registration process with the Network Repository Function (NRF). NE needs to provide its service information to the NRF according to the specified network service profile, such as NE type, NE instance ID, IP address of NE and PLMN ID (used to be discovered by other PLMNs), etc. Among them, the network service profile can be regarded as the “network element registration template”. In the SBA, the CN control plane NEs communicate with each other using the TCP/HTTP 2.0 based service-based interface (SBI). **This also means that the NE registration information may be transmitted in plaintext, which will be exposed to the risk of data leakage [25].**

In case of data leakage, this NE may be maliciously attacked after successful registration. In addition an attacker can use the stolen NE key information to forge a malicious NE and initiate a registration operation to the NRF. Once the registration is successful it means that there is a malicious NE node in the 5G core network. All

data passing through this node can be accessed and exploited by the attacker at will, which can cause more damage.

2. Security Threats in NE Subscription and Discovery

After registration, NE will inform other NRFs about its state. When a qualified NE initiates registration, the NRF notifies the subscribing NE and the subscribing NE determines whether it needs to communicate with the newly registered NE in the current period according to the actual service demand. The process of matching the newly registered NEs and updating the network element relationship is called "Discovery". **An attacker can use a man-in-the-middle attack or DoS attack to disrupt the communication between NEs and NRFs; 3GPP has discussed this problem in TS 33.501.** Three of them are worth being maliciously exploited by attackers as follows:

- The attacker performs a replay attack on the NRF, repeatedly initiating NE discovery or subscription requests to occupy NRF computing resources.
- The attacker can hijack the TCP session between the NE and the NRF, initiating unnecessary NE service subscription requests to the NRF by tampering with the NE's subscription request data, resulting in a waste of resources.
- The attacker can launch a DoS attack on the NRF to block the notification messages it sends to the subscribing NE. This causes the subscribing NE to remain in a state of expectation for one or more classes of network element services, which in turn may cause some service requirements of that subscribing NE to remain unavailable.

3. Security Threats in NE Logout

CN-NE will initiate a request to the NRF to go offline after ending its own service tasks. The NRF will delete the configuration data related to the logout NE after receiving the request. **The security problem in this phase is the data leakage caused by incomplete deletion of the data related to the logout NE [6].**

The residual NE configuration information may be mistaken as valid data by the NRF, which may affect NRF service operation. In addition, once the residual data is leaked, malicious attackers can utilize it to forge illegal NE registration requests, which can lead to DoS attacks.

4.1.2. Threats on NE Deployment of UPF Sinking

5G networks have a variety of application scenarios, and to ensure that slices can flexibly respond to the complex and diverse service demands, one of the core NEs in the control plane, the User Plane Function (UPF), should be deployed closer to the end user or at a decentralized location [25].

The UPF is mainly responsible for routing and forwarding packets in the data plane of the 5G core network and all core network data must be forwarded by the UPF to flow to the external network. The UPF is sunk to the network edge, which can reduce transmission delay, realize local shunting of data flow and relieve the data transmission pressure of the core network. It improves the network data processing efficiency, which in turn meets the vertical industry's demand for ultra-low latency, ultra-high bandwidth and security of the network.

However, the security threats introduced due to the sinking of UPF should not be underestimated. Among them, as the UPF is deployed closer to the wireless access network side, this exposes the control plane NE to a relatively low level of security protection. If the UPF is attacked (e.g., denial-of-service attacks on the UPF by malicious applications, tampering with the UPF configuration, etc.), the security issues that may result include data diversion policy conflicts on the UPF, signaling data overload, etc. and the entire core network control surface can even be affected. Tang et al. [42] describes two security threats that exploit security vulnerabilities in the Packet Forwarding Control Protocol (PFCP) to affect the normal operation of the UPF.

- Packet processing settings are tampered with. An attacker sends a session modification request containing the DROP flag in the "Apply Action" field of the forwarding action

rule. If the modification is successful, the UPF will delete the rule containing the TEID and the IP address of the base station, resulting in the GTP tunnel for the user’s downlink data being cut off and the user will not be able to access the Internet.

- The attacker can use the session modification request to redirect user traffic from the UPF to a resource under the attacker’s control. To do this, the attacker needs to change the IP address in the outer header creation field and thus access the user’s downlink data without the user realizing that the traffic is being intercepted.

4.1.3. Threats on NE Deployment of CU/DU Separation

In 5G, the access network is reconfigured and virtualized into the following three functional entities: the Centralized Unit (CU), Distribute Unit (DU) and Active Antenna Unit (AAU). The AAU connects to the DU part called 5G Fronthaul, the Middlehaul refers to the DU connecting to the CU part, and the Backhaul is the communication bearer between the CU and the core network.

In Figure 9, we identify the possible attack points that can be exploited in different deployment scenarios of CU/DU. When CU/DUs are deployed together, the attack mainly occurs in the transmission process between the access machine room and the core network. When the CU and DU are deployed separately, the control information between the two may not be protected by traditional security mechanisms. Attackers can launch attacks on the transmission path of the two communications for purposes such as stealing or tampering with data. In actual deployment, the correspondence principle between CU and DU is usually that a CU corresponds to one or more DUs. If an attacker attacks a CU that corresponds to more than one DU, then all the DUs connected to it are under the threat of being attacked.

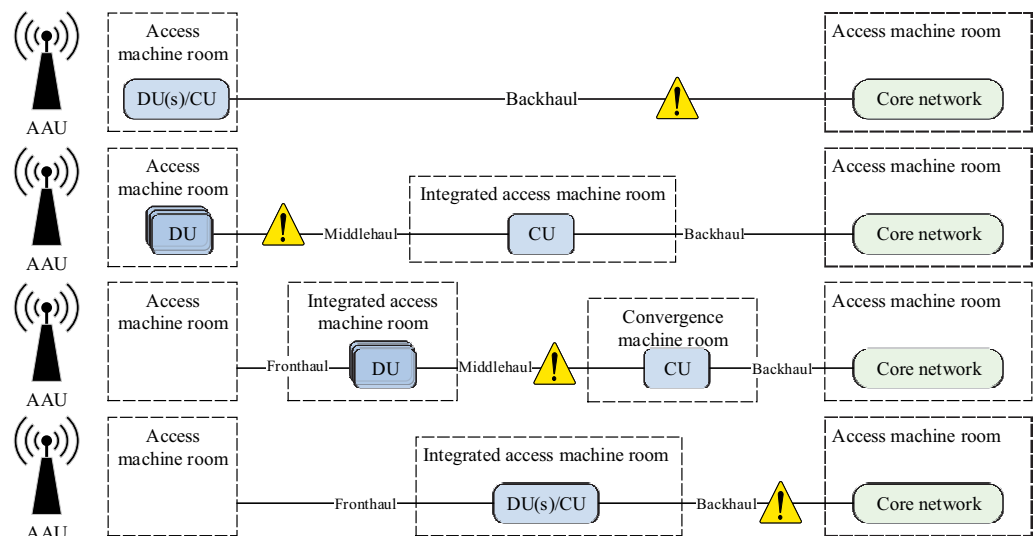


Figure 9. Multiple network deployment forms for CU/DU.

4.2. Security Issues in Slice Generation

The success of slicing deployment means that the 5G operator has the ability to provide logical “one-to-one” communication services to subscribers. When a subscriber initiates a request for a slicing service, the operator triggers the slicing generation process. This subsection summarizes the security threats in the process (see Figure 10).

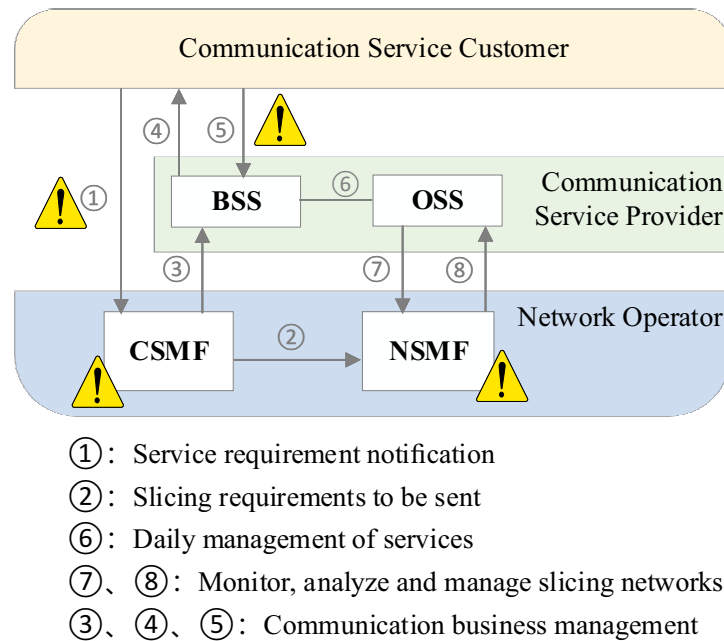


Figure 10. Security threats in the slice generation process.

4.2.1. Malicious Tampering with User Requirements

An attacker can perform a man-in-the-middle attack to maliciously tamper with a user's service requirements before the requirements reach the CSMF. When this malicious slice request reaches the CSMF and triggers the entire process of slice generation, this unreasonable slice request may lead to slice resource allocation confusion or malicious slice creation.

4.2.2. CSMF Permission Hijacking

As can be seen from the slicing management framework in Section 3, user slicing requests need to be sent to the CSMF for analysis and simplification first to obtain the corresponding parameterized network slicing requirements. The above process is referred to as the "capability negotiation process" in [27] and requires a standardized security protection for the whole negotiation process. We conclude that the following security threats exist if the negotiation process is not secured.

- The attacker attacks to infiltrate the CSMF and seize control of the CSMF before the user's slice request arrives. When the user request arrives at the CSMF, the attacker can steal the user's private data and cause a data breach. Or the attacker can use the stolen information to impersonate a legitimate user to initiate a slicing request to the 5G network, resulting in illegal theft of slicing resources.
- The attacker can launch a DoS attack on the CSMF or NSMF, causing the entire slice management module to go down. Subscriber services will not be satisfied or will always be down, potentially causing the telecom operator to lose a large number of 5G subscribers.
- The attacker launches an attack during the CSMF's analysis of subscriber requirements, misleading its CSMF to ignore or misunderstand the key information of subscribers, causing the subscriber requirements analysis to deviate and resulting in improperly designed slice templates. The service capability of all slices generated from that improper template is compromised.

4.2.3. Slice Template Information Leakage

The structure, configuration and subnetwork components contained in a 5G slice can be described by the Network Slice Template (NST) [12]. Jhanjhi et al. [7] suggest that the main point of attack in the slice creation process is the NST and, if the NST is

stolen by an attacker, all slices created with this template as reference will be affected. In addition, an attacker can maliciously allocate shared resources in the core network by means of tampering with the NST. This causes the slices to unconsciously occupy resources unreasonably, which in turn affects the resource allocation of the entire core network.

4.2.4. API Hijacking/Replay Attacks

In the slice generation phase, 3GPP TR 33.811 [27] identifies two public interfaces with security risks, i.e., the interface between the CSMF and the NSMF, and the interface between the Communication Service Provider (CSP) and the Communication Service Customer (CSC). Subscribers inform the operator network about their service requirements through the open interface managed by the CSMF and the CSP. The NSMF of the operator's network creates network slicing instances for the subscriber accordingly based on the subscriber's service requirements. The security threats against the public interfaces described in the document can be divided into three categories as follows.

- Attacks on the public interface to gain access to the slice (or communication service) management module. During the slice generation phase, external operators can access the slicing management module through the northbound standardized API [43]. Operators can perform different operations in different scenarios, such as creating or deleting slices, configuration, activation and monitoring of different levels of slices, etc. An attacker can interfere with slice configuration and activation, and thus the creation, instantiation and decommissioning process of a slice (or communication service) [18], by attacking the API. Examples include modifying existing slice configurations or deleting activated slices to cause denial of service, modifying slice routing configurations to cause malicious route targeting and potentially denial of service (or malicious charging) of slices (or communication services).
- Replay legitimate messages on public interfaces. The slice (or communication service) management module receives replayed legitimate messages and then unconsciously performs repeated management operations, such as repeated slice creation, repeated billing resulting in false charging, etc.
- Destroying the message integrity and authenticity of packets before they reach the interface. By tampering with the request information of a slice (or communication service), the attacker may create network slices that require a large amount of network resources (or network sub-slices) to support in order to exhaust the network resources and cause the network to go down.

4.3. Security Issues in Slice Operation and Maintenance

When a 5G slice is activated and instantiated, the slice enters its service phase. During this period, a large amount of slice operation data will be generated, accompanied with frequent access interface behaviors. In addition, we also focus on security threats specific to this operation phase, such as "multi-slice/multi-tenant" scenario security, AMF redirection security and endpoint security, etc. We mark these possible security threats in Figure 11.

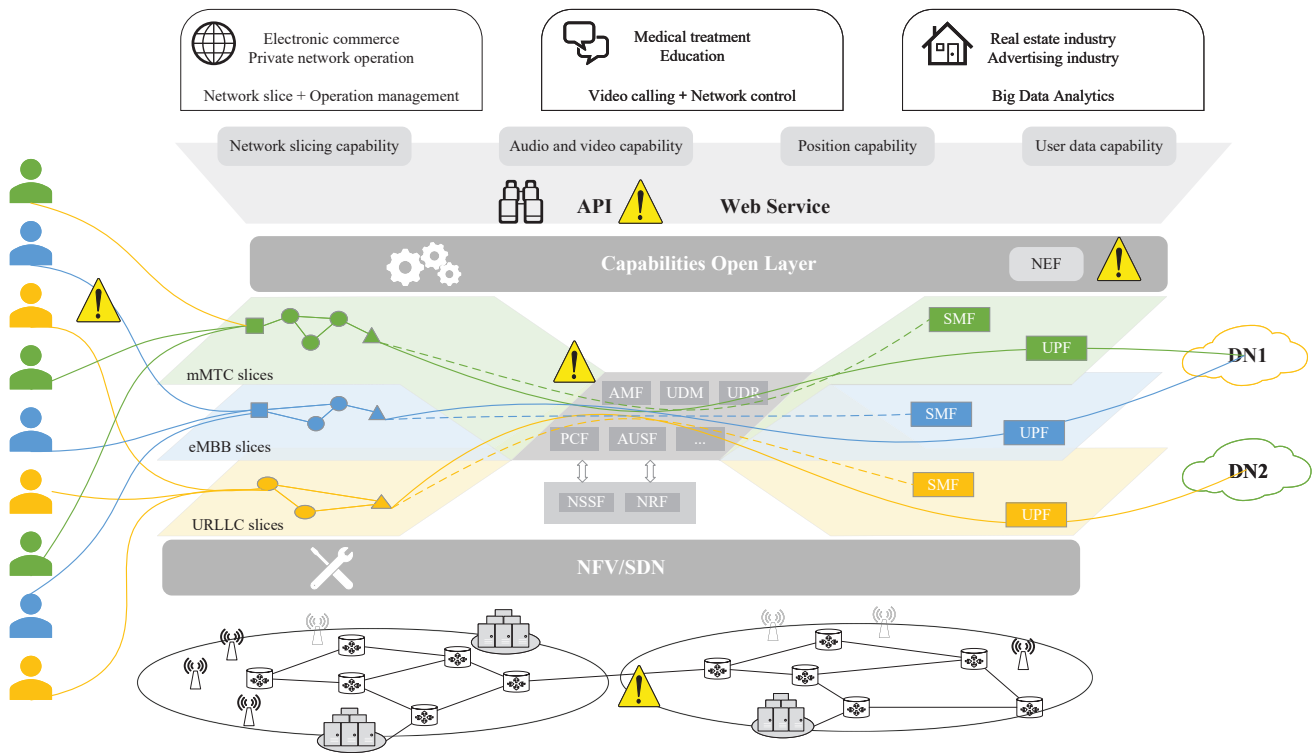


Figure 11. Security threats during slice operation and maintenance.

4.3.1. Threats on Management Data Leakage

In the period of slice operation and maintenance, a network slice is ready to be used and the Slicing Management System (SMS) needs to monitor and protect the slice. One of the essential functions of the SMS is to protect those sensitive data during the utilization of network slices, which relates to network slice selection information, the network slice operation monitoring report and network slice decommissioning information. An attacker may spoof these sensitive data and break the security of 5G network slices.

1. Threats over network slice selection information

To achieve error-free identification of end-to-end network slices, the current solution is to uniquely identify each network slice through Single Network Slice Selection Assistance Information (S-NSSAI). The presence of S-NSSAI simplifies the authentication process for user terminals to access each subnetwork slice of 5G and makes the matching of radio access network sub-slices with core network sub-slices more flexible. In addition, the ensemble consisting of one or more S-NSSAIs is called the Network Slice Selection Assistance Information (NSSAI). Among them, 3GPP specifies different types of NSSAIs for managing a subscriber’s slice signing information and slice request information. **It follows that the NSSAI requires a higher level of data security protection when a slice with service capability is requested to be put into use by a user**, i.e., when the slice is in the operational state.

3GPP TR 33.811 [27] points out that, if the confidentiality of the NSSAI is not guaranteed, the network slicing service will be exposed to data leakage and man-in-the-middle attacks at the connection establishment stage may happen. Assuming that the NSSAI is transmitted without encryption, an attacker could attempt to steal users’ private data. Further more, attackers can use the user’s privacy data to perform a man-in-the-middle attack on critical services related to the NSSAI to make the slicing services inoperable. There is also a data tampering attack against the rejected NSSAI specified by 3GPP, when an attacker performs data tampering on the rejected NSSAI so that the slice that needs to be revoked to be denied remains in an inaccessible state even if the user has legitimate access to the slice [27].

2. Threats over slice operation monitoring report
SMS uses the “slice operation monitoring report” to manage the operation status of the corresponding slice; the relevant configuration of the slice is modified according to the feedback of the monitoring report. **The confidentiality of the slice operation monitoring report can, to a certain extent, guarantee the safe operation of the slice.** Once the monitoring report is compromised, the slice operation information (e.g., topology information) within the valid time period of the report will be at risk of malicious exploitation [27]. Tampering with the slice operation data in the monitoring report misleads the slice management system to perform improper operations on the relevant slices, e.g., early retirement of slices, duplicate requests for slice sensitive resources, etc. The attacker can also collect a large number of slice operation monitoring reports to extract the operation characteristics of a class of slices and construct fake slices to achieve the purpose of disrupting the slice management system and obstructing the normal operation of legitimate slices.
3. Threats over network slice decommissioning information
The main work of the slice decommissioning phase is to release the slice resources and delete the slice-related information, which leads to the potential risk of leaking sensitive data exposed in the decommissioning process [14]. Moreover, since the slice decommissioning is essentially the process of resource release, when the resource release is not legitimate or the resource release is not complete, an attacker can launch a DDoS attack by consuming the current resources [18].

4.3.2. Threats on Opened Interfaces

In the period of slice operation and maintenance, how to use these network slicings well to solve real problems has become the main topic. In order to enhance the user experience, improve the scalability and flexibility of 5G slices, 3GPP added the Network Exposure Function (NEF) into the 5G core network to interact with third-party service providers. It acts as an interface between the 5G network and external entities, providing API-based access to network resources [15]. This idea can also be achieved by using “Cloud-native 5G Architecture”, which designs and implements the network functions and services as containerized micro-services [28]. In this case, the 5G core network can have open service interfaces to facilitate the integration of applications and service programs. Those opened APIs may also lead to security threats.

1. Threats in Opened Interfaces of NEF
NEF opens the network capabilities of the 5G core network to third-party applications to achieve a friendly interface between network capabilities and service requirements. In turn, it improves the service experience and optimizes the network resource allocation [44–46]. The northbound NEF network elements are open API interfaces for interfacing with third-party applications and the rest are southbound interfaces for interfacing with the 5GC. This shows that the open network capability of the 5G core network to the outside world is based on the secure communication of the northbound API interfaces of NEF. It also determines that the interaction process will face security issues such as data leakage, illegal authorized access, packet hostage, denial of service and shared data tampering.
2. Threats in Opened Interfaces of Cloud-native 5G Architecture
In a cloud-native 5G architecture, the network functions and services are designed and implemented as containerized micro-services, which can be dynamically orchestrated and managed in a cloud environment. When 5G core networks are deployed virtualized in the cloud, a number of security issues regarding remote management become particularly salient. Lingshu et al. [28] point out that cloud-based 5G core networks employ many open APIs, which makes it easier for attackers to exploit vulnerabilities and backdoors to illegally access unauthorized resources and consume more resources. In addition, attackers can launch various attacks to compromise the network slices by manipulating, managing and modifying the interfaces [29].

It is important to note that the key security threats to cloud-deployed 5G core networks will not be limited to interface security. Misconfiguration Vulnerabilities, Vulnerability of Applications and Malware Injection Attacks, etc. have also been discussed [24].

4.3.3. Threats in “Multi-Slice/Multi-Tenant” Scenarios

In 5G networks, multi-slice/multi-tenant scenarios refer to the capability of dividing the network infrastructure into multiple logical slices or virtual networks to support different services, applications or tenants. Each slice or tenant is allocated dedicated resources and customized network configurations to meet specific requirements and ensure isolation.

In order to achieve such scenarios, a series of complex interactions between network slices and various network objects (i.e., sub-slices, slices, user terminals, etc.) should be implemented. This also indicates that there must be resource sharing, multi-line access to parameters, and authorization of function calls among multiple slices or multiple tenants. As a result, a wrong interaction process can trigger an “avalanche” of damage to the operation of a slice. We analyzed such slicing security threats from three perspectives: terminal access slicing scenarios, multi-tenant scenarios and multi-slicing scenarios.

1. Threats in Terminal Access Slicing Scenario

In reality, the security landing point of network slicing and mutual authentication of user terminals are not the same. First of all, the key to the authentication of users by network slicing lies in the legitimacy and authenticity of users. Avoiding attackers can try to access the slice by impersonating legitimate users, resulting in illegal use of the slice service. Second, the key to user authentication for the slice lies in the integrity and reliability of the slice. Suppose a user accesses an incomplete slice that suffers from corruption; the user’s demand will not be responded to and at the same time the user may unknowingly send sensitive data to this malicious slice, thus it may lead to user data leakage.

Borgaonkar et al. [30] point out a logical vulnerability in the 5G Authentication and Key Agreement (5G-AKA) protocol specification, namely: the protection mechanism for sequence numbers (SQNs) is not secure under specific replay attacks due to its use of iso-or (XOR) and lack of randomness. Based on this vulnerability, Bello et al. [31] propose an attack against user location privacy.

2. Threats in Multi-tenant One-Slice Scenario

When multiple users rent the same network slice, the leased shared slice can be seen as a security weakness in the slicing service. Tenants who have a lease management relationship with the slice may try to access the private data of other tenants through the shared slice, resulting in data leakage. In addition, illegal changes to the shared parameters in the shared slice can cause the shared slice to fail to serve properly, thus making the shared slice a malicious node.

3. Threats in Multi-slice Scenarios With Single Tenant

The multi-slice scenario with single tenant is recognized in that the slices involved in the collaboration are all legitimate operational slices for that user. Since 3GPP proposes that a single user can only access up to eight network slices at the same time [15], this also indicates that this scenario is a slice collaboration with extremely limited slice resources. **Thus, we argue that the multi-slice collaboration with single tenant scenario is very sensitive to service requests and weakly fault-tolerant.**

Assuming that one of the user’s slices is attacked by a small amount of traffic, due to the limited service capacity of the slices, while prioritizing the normal operation of the slices themselves, the slices with which they have collaborative relationships may not be able to answer the requests. In addition, once one of the user’s slices is compromised, the collaborating slices will face the situation that no other slices are available for emergency response, which will lead to the paralysis of the collaborating slices’ services.

4. Threats in Multi-slice Scenarios With Multiple Tenants

A multi-slice scenario with multi-user participation is a situation where network sub-slices from different security domains (users or slices with different security levels) collaborate with each other. Olimid et al. [6] propose that, if a slice is defined as a “sub-slice chain” formed by multiple sub-slices, the interconnected nodes in the chain may become points of attack. **The overall security level in a sub-slice chain depends on the least secure sub-slice in the chain.** The attacker may try to attack the sub-slice with a low security level (especially the RAN sub-slice) to reach the sub-slice with a higher security level [14,32], which is located in the same sub-slice chain.

In a connected vehicle scenario, since passengers or drivers may have different service requirements, vehicles can be connected to multiple slices simultaneously to satisfy various service requirements [33]. However, these services may have different security levels, which also leads to two types of security threats for such multi-slice communication, namely cross-slice data leakage and malicious exploitation of inter-slice communication. Assuming that a vehicle receives sensitive data from one slice and also uses data from another slice with a lower security level, such cross-slice multi-slice data access can lead to data leakage. More seriously, such cross-slice security threats are made more severe due to the high mobility of vehicles [39].

Some of the same security threats exist in both multi-slice scenarios. For example any DDoS attack against one slice may result in the compromise of other slices with which it shares physical resources. Similarly, if communication links are shared among multiple slices, then an attack on one slice may affect other slices [34]. An attacker may use inter-slice communication as a bridge to attack certain functions in a slice and disrupt related functions in other slices with which it has a communication relationship [33].

In addition, there are several slice managers in 5G networks that are responsible for the creation, scheduling and instantiation of slices. Khan et al. [35] propose that, when multiple slice managers coexist, they must authenticate each other, otherwise there is no way to guarantee the security of users when they access multiple slices (belonging to different slice managers) and the reliability of inter-slice communication. When multiple slices allow inter-slice communication, possible security threats include unauthorized access, sensitive data leakage from inter-slice transfers and shared parameter leakage (if any) [36].

4.3.4. Threats in AMF Redirection

The Access and Mobility Management Function (AMF) is a central node where most of the control plane functions (e.g., UDM, AUSF, etc.) of 5GC need to interact with it, and it is also the operational hub of the 5GC sub-slices. When using the network slices, a slice user may move from one location area to another and needs to be served by a different AMF, which will cause the AMF redirection procedure. This means that sensitive slice data may pass through some unauthorized AMFs and its security needs to be guaranteed.

3GPP TR 33.813 [37] presents a security threat caused by the non-separation of AMF keys. When the AMF (source AMF) initially selected by the 5G network around for the user cannot serve the user slice or cannot support the change of the slice function, the 5G network will trigger the AMF redirection mechanism or select a suitable AMF (target AMF) from the existing AMF set for replacement. It is worth noting that, once a change in AMF occurs, the target AMF needs to update the entire key hierarchy of the source AMF, i.e., key separation. Assuming that no key separation is performed, the source AMF and the target AMF will be mutual sources of key exposure, and data confusion may occur for the different slices existing on these two network elements. At the same time, there will be a risk of leakage of sensitive user data on the related AMFs.

4.3.5. Threats from Terminal User

After the slice is normally put into use, the biggest security threat affecting the normal operation of the slice lies in the terminal user. On the one hand, due to the variability

in terminal equipment hardware, the security solution designed by operators for slicing cannot be compatible with the security requirements of all hardware; secondly, the direct or indirect users of slicing are biological entities with independent minds and certain operational capabilities. This leads to a large portion of security threats to slicing being triggered by improper user operations or users using slicing in an insecure environment.

Dhamija et al. [38] suggest that, if the end users of slices are human, they are more likely to fall victim to ransomware attacks or advanced phishing attacks and spoofing techniques, leading to threats to slicing security. In multi-tenant coexistence networks in 5G core networks, an adversary may steal sensitive information (e.g., passwords or keys) by exploiting side channels to bypass the logical separation between dockers [47]. Alliance et al. [32] point out that a hostage end device may excessively consume the shared resources in the slice to which it has access, which in turn may disrupt the performance of the slice or even successfully perform a DoS attack. The security risks associated with 5G client devices increase when they access network slices over non-3GPP networks [14].

In the IoT scenario, end hardware devices are vulnerable to various security attacks because the slicing tenant is a weak security entity. If the terminal hardware is not properly protected, they can be contaminated by malware or turned into puppets in DDoS attacks. In addition, they can be affected by hardware tampering or sensor errors, and, in this case, compromised end devices may even inadvertently continue to allow inter-slice communication, thus extending the impact of the attack [48].

4.3.6. Threats on Physical Layer

The physical layer, as the underlying resource base of the 5G network slicing architecture, may be subject to attacks such as exhaustive attacks, denial of service and software attacks. It is worth noting that attacks against the resource layer usually have a certain degree of chain transmission. When an attacker tampers with the source code of a slice, this results in compromising the related functionality of all slices that use that source code [32]. Wang et al. [39] state that an attacker can use a tenant endpoint as an entry point. The physical resource or infrastructure is compromised by means of resource consumption, malware implantation or even physical attacks, thus causing all slices built on that resource to be affected. In addition, an attacker can also exploit a vulnerability in the VM monitor program to gain root privileges and all containers assigned on this VM monitor system are likely to be attacked, causing the slices to fail to function properly [28]. Some experienced attackers can launch a Basic Input/Output System (BIOS) attack, which in turn can directly threaten the physical server [40].

The physical layer is also at risk from side-channel attacks. Since multiple slices in a 5G network may share various underlying physical resources, if an attacker can observe (power consumption, uptime, etc.) or affect the operation of a slice's functionality, they may also affect another slice that shares physical resources with that slice, or obtain some operational information, keys or other private information of the vehicle user [32]. Especially when the security level of the target slice is high, side-channel attacks can be effective attacks [39].

5. Requirements and Recommendations for Creating 5G Network Slicing Systems

In the last section, we systematically analyzed the potential security threats in different phases of the 5G network slicing lifecycle and discussed the existing security enhancing solutions corresponding to each threat. However, these existing solutions usually focus on one threat or parts of threats on 5G network slices, to build a secure 5G network slicing system we need to consider more comprehensive scenarios. In this section, based on the results achieved in the last section, we summarized a general security requirement/principle list and give our recommendations for creating 5G network slicing in Figure 12 which connects the requirement together with the related threats (Table 1) to identify the traceability of each other.

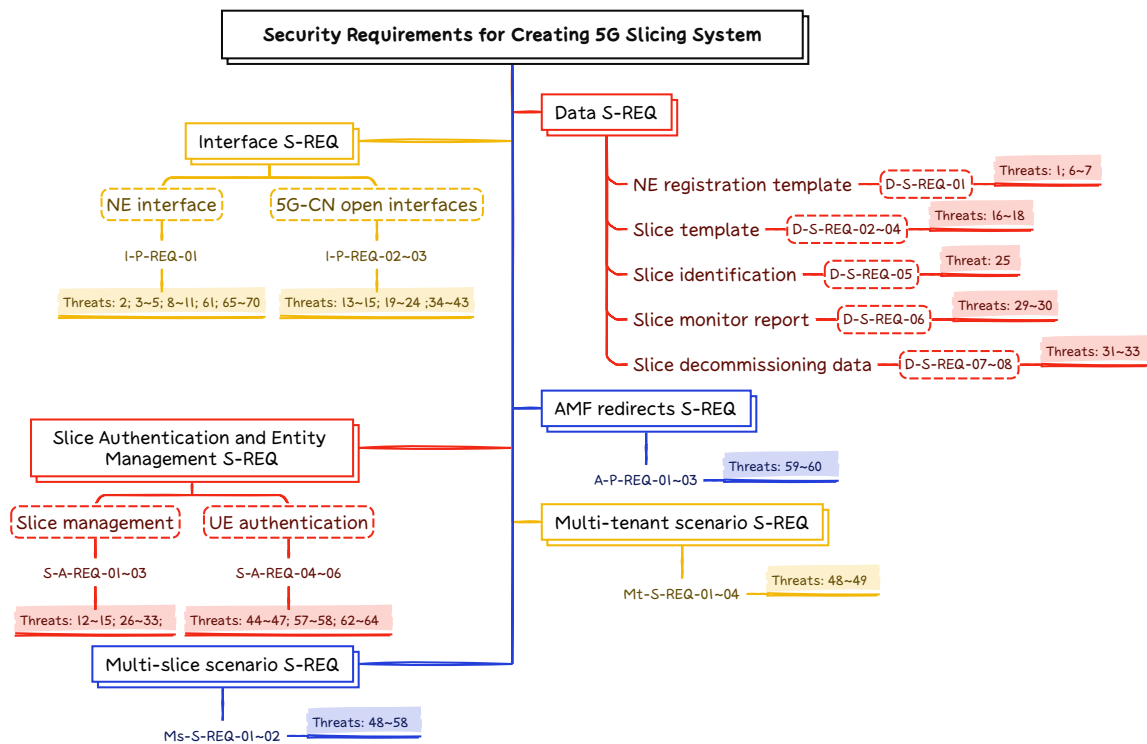


Figure 12. Security requirements and recommendations for creating 5G network slicing system.

5.1. Data Security Requirements and Recommendations

Regarding the analysis results in last section, we found that many security threats to 5G network slicing are caused by the incorrect using or configuring of the control data. For example, in the 5G network slicing deployment and generation phase, protecting template security becomes the primary requirement for slicing data security; in the slice operation phase, slice identification and the slice operation report are also the focus of data protection; in the slicing decommissioning phase, the decommissioning resources and sensitive data require certain security handling solutions. We summarize the specific data security requirements of 5G network slices as follows:

Security Requirements:

- **D-S-REQ-01:** NE Registration Template shall have data confidentiality and integrity protection mechanisms;
- **D-S-REQ-02:** Slice templates shall be protected against detection and confidentiality mechanisms;
- **D-S-REQ-03:** Slice templates shall be checked for correctness and completeness prior to use;
- **D-S-REQ-04:** Slice templates should be dynamically adjusted and optimized;
- **D-S-REQ-05:** Temporary slice identification shall be updated periodically;
- **D-S-REQ-06:** Slice monitoring reports shall have a data confidentiality and integrity protection mechanism;
- **D-S-REQ-07:** Decommissioning slice data should be desensitized;
- **D-S-REQ-08:** Decommissioning slice resources should have a “cooling-off period”.

Recommendations: From a perspective of 5G system construction, not all of the listed security requirements need to be met at first. We classified the importance of the above data security requirements and give the following recommendations. Firstly, as operators must develop standardized data encryption and protection algorithms during network slicing deployment, generation and management, the D-S-REQ01 and D-S-REQ06 are classified as “especially important”, i.e., operators need to be mandated to meet this requirement. Secondly, for slice-sensitive data (temporary slice identifiers, slice decommissioning data,

etc.), operators can selectively fulfill the slice security requirements of users, so D-S-REQ04, D-S-REQ05 and D-S-REQ08 are classified as “important”. Finally, D-S-REQ02, D-S-REQ03 and D-S-REQ07 can be provided as the operator’s special slicing security service to meet the security requirements of slicing data in different slicing application scenarios, i.e., “optional” (see Table 3).

Table 3. Data security recommendations.

Security Requirements	Security Recommendations
D-S-REQ-01	especially important
D-S-REQ-02	optional
D-S-REQ-03	optional
D-S-REQ-04	important
D-S-REQ-05	important
D-S-REQ-06	especially important
D-S-REQ-07	optional
D-S-REQ-08	important

5.2. Interface Protection Requirements and Recommendations

The essence of a 5G network slice operation is the mutual collaboration among VNFs within a 5G network, so the security of communication interfaces between VNFs is directly related to the secure operation of the slice. 5G network operators can demonstrate new features to vertical service providers through APIs [49]. The security requirements for the interfaces are summarized as follows:

Security Requirements:

- **I-P-REQ-01:** Reliable transmission between NE interfaces shall be established using TLS as the authentication mechanism and OAuth 2.0 as the authorization protocol;
- **I-P-REQ-02:** The 5G-CN external interface shall authenticate and authorize third-party applications;
- **I-P-REQ-03:** The 5G-CN external interface should have the capability of security auditing, monitoring, analysis and reporting [43].

Recommendations: Among the above interface security requirements, we classified I-S-REQ01 and I-S-REQ02 as “especially important”, i.e., the relevant interfaces of the network slices must have authentication and authorization capabilities in reality. In addition, I-S-REQ03 can be used as a featured security attribute of the slice interface to serve slices with higher security demands, i.e., “optional” (see Table 4).

Table 4. Interface protection recommendations.

Protection Requirements	Protection Recommendations
I-P-REQ-01	especially important
I-P-REQ-02	especially important
I-P-REQ-03	optional

5.3. AMF Redirection Protection Requirements and Recommendations

3GPP TS 33.501 [26] proposes a scheme to guarantee forward and backward security during AMF changes. When AMF redirection occurs, based on the local operator policy, the source AMF can derive a new key for the target AMF and the target AMF should trigger a new authentication process with the user. The new authentication process can refresh the whole key hierarchy and achieve complete blocking of the communication between the UE and the source AMF, which guarantees the forward and backward security of the AMF. The security requirements are summarized as follows:

Security Requirements:

- **A-P-REQ-01:** The source AMF shall export a new key for the target AMF;

- **A-P-REQ-02:** The target AMF shall trigger a new authentication process with the user;
- **A-P-REQ-03:** The new authentication process shall refresh the entire key hierarchy.

Recommendations: Once the 5G network slicing system supports roaming, we think all of the AMF redirection protection requirements should be “especially important”. These security requirements must be met in order to provide better forward and backward security in the event of an AMF redirection on a slice (see Table 5).

Table 5. AMF redirection protection recommendations.

Protection Requirements	Protection Recommendations
A-P-REQ-01	especially important
A-P-REQ-02	especially important
A-P-REQ-03	especially important

5.4. Slice Authentication and Entity Management Requirements and Recommendations

In order to meet the more stringent security requirements of some vertical service providers, 3GPP introduced the concept of “secondary authentication”, i.e., primary and secondary authentication [26]. 3GPP TS 23.501 [15,37,50] suggests that secondary authentication (or slice specific authentication) should be performed at the slice level and that secondary authentication should be in charge of the entity management issues of the slice. The specific security requirements are listed as follows:

Security Requirements:

- **S-A-REQ-01:** Network operators shall periodically perform a trusted assessment of the slice management module;
- **S-A-REQ-02:** The slice management module shall have two-way authentication with the slice user;
- **S-A-REQ-03:** The slice management module shall check the authenticity and completeness of the user’s slice request;
- **S-A-REQ-04:** Slice users should be primary authenticated;
- **S-A-REQ-05:** Third-party service providers shall have the right to require secondary authentication of slice users;
- **S-A-REQ-06:** Specific slices should require user authentication and authorization at the slice level.

Recommendations: Regarding the above security requirements, we classified S-A-REQ02 and S-A-REQ04 as “especially important”, which ensure that users can legitimately request and access the slices, and they are the security basis for the normal operation of the slice. The rest of the security requirements (S-A-REQ01/03/05/06) can be satisfied by the users themselves, i.e., “optional”. If all of them are satisfied, it can improve the anti-attack ability of users when using slices; on the contrary, not satisfying them will not affect the normal and safe operation of slices (see Table 6).

Table 6. Slice authentication and entity management security recommendations.

Security Requirements	Security Recommendations
S-A-REQ-01	optional
S-A-REQ-02	especially important
S-A-REQ-03	optional
S-A-REQ-04	especially important
S-A-REQ-05	optional
S-A-REQ-06	optional

5.5. Multi-Tenant Scenario Security Requirements and Recommendations

5G network slicing enables multiple tenants to be able to share the same physical resources. Valero et al. [51] state that multi-tenant scenarios should focus attention on

security and risk management in multi-slice domains. 3GPP recommends network slice performance and fault monitoring in multi-tenant environments [52]. Odarchenko et al. [53] proposed a security assessment index and method that can be used in 5G network slicing systems. This method can conduct security monitoring for special user groups and achieve the reliable operation of multi-tenant slicing services. The security requirements are summarized as follows:

Security Requirements:

- **Mt-S-REQ-01:** Slice users should have privacy protection mechanisms [25];
- **Mt-S-REQ-02:** Multi-tenant slices should have performance monitoring and fault detection mechanisms.

Recommendations: In multi-tenant scenarios, we consider Mt-S-REQ01 and Mt-S-REQ02 to be “especially important”; however, simply implementing them cannot guarantee secure operations in multi-tenants scenarios. We suggest that users can combine Ms-S-REQ01 and Ms-S-REQ02 with the “important” and “optional” data/interface security requirements to form a more robust slicing security solution (see Table 7).

Table 7. Multi-tenant scenario security recommendations.

Security Requirements	Security Recommendations
Mt-S-REQ-01	especially important
Mt-S-REQ-02	especially important

5.6. Multi-Slice Scenario Security Requirements and Recommendations

Network slicing is a virtualization, containerization and software-defined networking-based technology. Faults and errors in one network slice can be propagated to other network slices through the virtual environment, and attackers may span network slices to abuse the network for their desired purposes [2]. Currently, an important tool to address security issues in multi-slice collaboration scenarios in 5G networks is slice isolation [54]. The security requirements to achieve slice isolation are listed below:

Security Requirements:

- **Ms-S-REQ-01:** Access networks shall introduce conflict avoidance protocols to achieve sub-slice isolation;
- **Ms-S-REQ-02:** Transportation of traffic shall be secured by the bearer network using physical/logical segregation;
- **Ms-S-REQ-03:** Core network elements should be segregated by security level;
- **Ms-S-REQ-04:** Different security domain network elements should develop strict security access authentication mechanisms.

Recommendations: Unlike multi-tenant scenarios, we considered the security requirements of multi-slice scenarios to be “optional”. The security issues in multi-slice scenarios were diverse and composite. A single security requirement cannot effectively guarantee the secure operations of multiple slices. Therefore, we suggested that, in multi-slice scenarios, multiple security requirements should be combined to form a comprehensive and systematic slice security operation scheme based on the characteristics of the scenario (see Table 8).

Table 8. Multi-slice scenario security recommendations.

Security Requirements	Security Recommendations
Ms-S-REQ-01	optional
Ms-S-REQ-02	optional
Ms-S-REQ-03	optional
Ms-S-REQ-04	optional

6. Future Trends in 5G Network Slicing Security

The 5G network slice serves as a key hub connecting users and service providers, which can forward and process massive amounts of communication data. It is also the primary gateway for user authentication and access control. At this point, it is very important to make reasonable use of artificial intelligence and Zero Trust to assist 5G network slices in analysis and authentication. In this regard, we have investigated the existing research and given an outlook on future research trends. In addition, as the research on 6G networks progresses, network slicing technology will also face great challenges. In this regard, we have conducted research on related studies and an outlook on future research trends.

6.1. Artificial Intelligence

The original intention of 5G network slicing is “scene personalization” to achieve the “Internet of everything”, which also predicts that the implementation of 5G slices will be accompanied by massive data generation with certain scene characteristics. Under the premise of massive data guarantee, 5G network slicing scenarios are gradually receiving attention from AI-related research and applications, and the potential of using machine learning means to ensure the security of slicing is also increasingly evident. AI and ML technologies manage, enhance and distribute network slices within 5G networks, a process known as AI/ML-assisted network slicing [55,56]. As technologies advance, mechanisms based on reinforcement learning are being developed to ensure the security of network slices [57].

Thantharate et al. [58] secure slicing network load efficiency and availability by means of deep learning (DL) neural networks, and the data set for model training is derived from network key performance indicators (KPIs). The model is simulated by performing scenarios in which slicing failures occur and the final results show that the model can guarantee the availability of the network in case of slicing failures to some extent. Sedjelmaci et al. [59] propose a hierarchical detection scheme based on a reinforcement learning process to ensure the safe operation of end-to-end 5G network entities and thus the service security of 5G end-to-end network slices. Thantharate et al. [60] propose a neural network-based “5G security” network slicing model from the user’s perspective to proactively detect and eliminate incoming threats before they attack the 5G network.

In terms of the current application of AI technologies in 5G network slicing security scenarios, we can find that most researchers focus on developing relevant software security platforms using historical slicing traffic data. In addition, relevant research is also devoted to the analysis of data such as slice access or user access cell switching, i.e., the research focuses on the slice security of the radio access network side. In summary, there are relatively few research solutions for 5G core network slicing security issues and there is a lack of research on real-time defense for slicing operations.

6.2. Zero Trust Model

The introduction of 5G mobile networks further promotes the transformation of social informatization from network construction as the core to data construction with the purpose of data usage and sharing. The corresponding network security construction also shifts from network boundary protection to data- and resource-centric security protection, which fits with the Zero Trust concept proposed by Forrester in 2010. Zero trust is a proactive security model. The model is based on entity device assessment and user authentication, and ensures that entities in cyberspace are free of malicious behaviors by continuously analyzing and verifying the trust relationships between them, thereby deterring and mitigating cybersecurity risks [61].

Carrozzo et al. [62] propose an initial concept of a zero-touch security and trust architecture for pervasive computing and connectivity in 5G networks, aiming to implement cross-domain security and trust coordination mechanisms. Dzogovic et al. [63] investigate the potential threat of DDoS and designs a solution based on the Zero Trust security model to ensure the continuity of services in the corresponding disaster scenarios. The Zero Trust

model applied to 5G network slicing security can reduce the overall operational complexity and enhance the security of network slicing systems [64]. However, Zero Trust does not solve all security problems in 5G network slicing [61].

The Zero Trust model can address the potential security issues of sliced systems for access between manageable users, endpoints and service resources. The Zero Trust model is not able to help when the access entity becomes a mass service. It is well known that 5G network slicing to take over public nature services is a general trend and the existing research on the Zero Trust model still needs to be deepened. The evaluation of the authentication and entity trust relationship in the model cannot be limited to small-scale collectives, and the focus should be put on the trust relationship of mass, universal and normalized public business as entities, and solving the large-scale security authentication problem is one of the main challenges in the 5G network slicing scenario.

6.3. 6G Network Slicing Security

As the commercial deployment of 5G networks continues to improve, the vision of “information interaction and connectivity for everything” is gradually being realized with the concentration of connected objects in the 10km height range on land. The convergence and coexistence of heterogeneous access networks with “full coverage” envisioned by 6G means that access network sub-slicing will face a more complex network internal slicing management and orchestration environment. The large number of heterogeneous access network nodes allows for more weak security entry points between the internal network and the outside world. In addition, the enhanced 6G supply and demand capability will increase the number of available services in the network, which will lead to a large number of network slices with different performance requirements, functions and time spans running in parallel, making slice isolation significantly more difficult. Meanwhile, resource sharing, data transmission and service collaboration in multi-slice scenarios will be exposed to higher attack risks.

It can be seen that the research into 6G slice security will be more challenging on the basis of 5G slice security. Most of the related research is at the theoretical stage, and Ramezani et al. [65] introduce the basic principles of the Zero Trust framework and point out the key requirements for integrating the Zero Trust principles into 5G/6G networks. The above study argues that 5G/6G networks incorporating the Zero Trust framework can use artificial intelligence algorithms to secure information in untrustworthy networks. An intelligent Zero Trust framework based on artificial intelligence conforming to 5G/6G access networks is proposed and the basic principles of how to achieve Zero Trust using existing artificial intelligence algorithms are discussed.

7. Conclusions

This paper is dedicated to summarizing and analyzing the security issues in the construction process of a 5G network slicing system at a fine-grained level. Firstly, we summarize the background knowledge of 5G networks and analyze the necessity of introducing slicing technology in 5G networks. At the same time, we consider that the application of network slicing technology will bring some unique security threats for 5G. Secondly, this paper introduces the basic concepts and management architecture of network slicing. After reviewing and organizing a vast body of literature, we detail the security threats associated with the deployment, creation and maintenance of slices in Section 4. Specifically, we address the security risks posed by unreliable user requirement analysis, advocating for robust interactions between the 5G network slicing management module and its users to ensure precise and secure requirement assessments. Consequently, we propose the development and implementation of targeted communication security protocols or signaling encryption algorithms tailored for various network functions and user groups.

In addition, we organized corresponding security requirements for different scenarios of 5G network slicing based on the sorting out of existing security threats. Meanwhile, from the perspective of securely building 5G network slicing systems, we classified the impor-

tance of security requirements in different scenarios. We suggest that operators should take “especially important” security requirements as mandatory service capabilities. Finally, we organized the future research trends of 5G network slicing security. We hope that this paper can help readers understand the latest development of 5G network slicing security, and provide more new ideas for future research on the safe and reliable deployment of network slicing technology in wireless communications.

Author Contributions: Conceptualization, S.G. and Y.F.; methodology, H.L.; validation, J.C. and R.L.; investigation, S.G.; writing—original draft preparation, S.G. and Y.F.; writing—review and editing, H.L., J.C. and R.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Key R&D Program of China No. 2022YFB2902205 and the Natural Science Basis Research Plan in Shaanxi Province of China (No. 2021JM137).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

3GPP	3rd Generation Partnership Project
5G	Fifth Generation Mobile Communications Technology
5GC	5G Core Network
AAU	Active Antenna Unit
AMF	Access and Mobility Management Function
API	Application Programming Interface
AUSF	Authentication Server Function
BIOS	Basic Input/Output System
BSS	Business Support Systems
CN	Core Network
CPU	Central Processing Unit
CSC	Communication Service Customer
CSMF	Communication Service Management Function
CSP	Communication Service Provider
CU	Centralized Unit
DDoS	Distributed Denial of Service
DROP	Data Retention Optimization Protocol
DU	Distributed Unit
DoS	Denial of Service
ETSI	European Telecommunications Standards Institute
GTP	GPRS Tunneling Protocol
KPI	Key Performance Indicator
MANO	Management And Network Orchestration
MDPI	Multidisciplinary Digital Publishing Institute
NE	Network Element
NEF	Network Exposure Function
NFV	Network Functions Virtualization
NFVI	Network Functions Virtualization Infrastructure
NFVO	Network Functions Virtualization Orchestrator
NRF	Network Repository Function
NSI	Network Slice Instance
NSMF	Network Slice Management Function

NSSAI	Network Slice Selection Assistance Information
NSSF	Network Slice Selection Function
NSSI	Network Slice Subnet Instance
NSSMF	Network Slice Subnet Management Function
NST	Network Slice Template
OSS	Operational Support Systems
PCF	Policy Control Function
PFCP	Packet Forwarding Control Protocol
PLMN	Public Land Mobile Network
QoS	Quality of Service
RAN	Radio Access Network
RPA	Robotic Process Automation
S-NSSAI	Single Network Slice Selection Assistance Information
SBA	Service-Based Architecture
SBI	Service-Based Interface
SDN	Software Defined Networking
SDNO	Software-Defined Networking Orchestrator
SMS	Slicing Management System
SQN	Sequence Number
TCP	Transmission Control Protocol
TEID	Tunnel Endpoint Identifier
TN	Transport Network
UDM	Unified Data Management
UDR	Unified Data Repository
UPF	User Plane Function
VIM	Virtual Infrastructure Manager
VNF	Virtual Network Function
VNFM	Virtual Network Function Manager
XOR	Exclusive OR
eMBB	Enhanced Mobile Broadband
uRLLC	Ultra-Reliable Low-Latency Communications

References

- Subedi, P.; Alsadoon, A.; Prasad, P.; Rehman, S.; Giweli, N.; Imran, M.; Arif, S. Network slicing: A next generation 5G perspective. *EURASIP J. Wirel. Commun. Netw.* **2021**, *2021*, 102. [\[CrossRef\]](#)
- Wong, S.; Han, B.; Schotten, H.D. 5G Network Slice Isolation. *Network* **2022**, *2*, 153–167. [\[CrossRef\]](#)
- Chen, Y.Z.; Chen, T.Y.H.; Su, P.J.; Liu, C.T. A Brief Survey of Open Radio Access Network (O-RAN) Security. *arXiv* **2023**, arXiv:2311.02311.
- Khan, L.U.; Yaqoob, I.; Tran, N.H.; Han, Z.; Hong, C.S. Network slicing: Recent advances, taxonomy, requirements, and open research challenges. *IEEE Access* **2020**, *8*, 36009–36028. [\[CrossRef\]](#)
- Dangi, R.; Jadhav, A.; Choudhary, G.; Dragoni, N.; Mishra, M.K.; Lalwani, P. MI-based 5g network slicing security: A comprehensive survey. *Future Internet* **2022**, *14*, 116. [\[CrossRef\]](#)
- Olimid, R.F.; Nencioni, G. 5G Network Slicing: A Security Overview. *IEEE Access* **2020**, *8*, 99999–100009. [\[CrossRef\]](#)
- Jhanjhi, N.; Verma, S.; Talib, M.; Kaur, G. A canvass of 5G network slicing: Architecture and security concern. *IOP Conf. Ser. Mater. Sci. Eng.* **2020**, *993*, 012060.
- Salahdine, F.; Liu, Q.; Han, T. Towards Secure and Intelligent Network Slicing for 5G Networks. *IEEE Open J. Comput. Soc.* **2022**, *3*, 23–38. [\[CrossRef\]](#)
- Dhanasekaran, R.M.; Ping, J.; Gomez, G.P. End-to-End Network Slicing Security Across Standards Organizations. *IEEE Commun. Stand. Mag.* **2023**, *7*, 40–47. [\[CrossRef\]](#)
- Singh, V.P.; Singh, M.P.; Hegde, S.; Gupta, M. Security in 5G Network Slices: Concerns and Opportunities. *IEEE Access* **2024**, *12*, 52727–52743. [\[CrossRef\]](#)
- Rost, P.; Mannweiler, C.; Michalopoulos, D.S.; Sartori, C.; Sciancalepore, V.; Sastry, N.; Holland, O.; Tayade, S.; Han, B.; Bega, D.; et al. Network slicing to enable scalability and flexibility in 5G mobile networks. *IEEE Commun. Mag.* **2017**, *55*, 72–79. [\[CrossRef\]](#)
- 3rd Generation Partnership Project (3GPP). Study on Management and Orchestration of Network Slicing for Next Generation Network. Technical Specification 3GPP TR 28.801 Version 15.1.0 Release 15. 2017. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3091> (accessed on 10 April 2024).

13. Ordonez-Lucena, J.; Ameigeiras, P.; Lopez, D.; Ramos-Munoz, J.J.; Lorca, J.; Folgueira, J. Network slicing for 5G with SDN/NFV: Concepts, architectures, and challenges. *IEEE Commun. Mag.* **2017**, *55*, 80–87. [[CrossRef](#)]
14. 3rd Generation Partnership Project (3GPP). Study on the Security Aspects of the Next Generation System. Technical Specification 3GPP TR 33.899 Version 14.1.0 Release 14. 2017. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045> (accessed on 10 April 2024).
15. 3rd Generation Partnership Project (3GPP). System Architecture for the 5G System and Stage 2. Technical Specification 3GPP TS 23.501 Version 16.6.0 Release 16. 2020. Available online: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf (accessed on 10 April 2024).
16. Groupe Speciale Mobile Association. An Introduction to Network Slicing. Technical Specification. 2017. Available online: https://www.etsi.org/deliver/etsi_ts/123500_123599/123501/16.06.00_60/ts_123501v160600p.pdf (accessed on 10 April 2024).
17. 3rd Generation Partnership Project (3GPP). Study on Architecture for Next Generation System. Technical Specification 3GPP TR 23.799 Version 14.0.0 Release 14. 2016. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3008> (accessed on 10 April 2024).
18. Hongyi, L.; Yirong, Z.; Jinyan, L.; Xuettian, Z. Research on 5G network slice management based on network exposure. *Dianzi Jishu Yingyong* **2020**, *46*, 1–5. [[CrossRef](#)]
19. Le, H.; Lei, X.; Baojun, J. 5G Network Slice Management System and Practice of CSPs. *Front. Data Comput.* **2020**, *2*, 44–54.
20. Jin-Wen, W.; Xiao-Li, Z.; Qi, L.; Jian-Ping, W.; Yong, J. Network Function Virtualization Technology: A Survey(Review). *Chin. J. Comput.* **2019**, *42*, 415–436. [[CrossRef](#)]
21. Yousaf, F.Z.; Bredel, M.; Schaller, S.; Schneider, F. NFV and SDN—Key technology enablers for 5G networks. *IEEE J. Sel. Areas Commun.* **2017**, *35*, 2468–2478. [[CrossRef](#)]
22. An, Q.; Liu, Y.; Sun, Q.; Tian, L. Network slicing architecture based on SDN and NFV. *Telecommun. Sci.* **2016**, *32*, 119b126.
23. Singh, J.; Refaey, A.; Shami, A. Multilevel security framework for nfv based on software defined perimeter. *IEEE Netw.* **2020**, *34*, 114–119. [[CrossRef](#)]
24. Jangjou, M.; Sohrabi, M.K. A comprehensive survey on security challenges in different network layers in cloud computing. *Arch. Comput. Methods Eng.* **2022**, *29*, 3587–3608. [[CrossRef](#)]
25. Zhang, S.; Wang, Y.; Zhou, W. Towards secure 5G networks: A Survey. *Comput. Netw.* **2019**, *162*, 106871. [[CrossRef](#)]
26. 3rd Generation Partnership Project (3GPP). 5G Security Architecture and Procedures for 5G System. Technical Specification 3GPP TS 33.501 Version 16.3.0 Release 16. 2020. Available online: https://www.etsi.org/deliver/etsi_ts/133500_133599/133501/16.03.00_60/ts_133501v160300p.pdf (accessed on 10 April 2024).
27. 3rd Generation Partnership Project (3GPP). Study on Security Aspects of 5G Network Slicing Management. Technical Specification 3GPP TR 33.811 Version 15.0.0 Release 15. 2019. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3358> (accessed on 10 April 2024).
28. Lingshu, L.; Jiangxing, W.; Hongchao, H.; Wenyan, L.; Zehua, G. Secure cloud architecture for 5G core network. *Chin. J. Electron.* **2021**, *30*, 516–522. [[CrossRef](#)]
29. Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A. Overview of 5G security challenges and solutions. *IEEE Commun. Stand. Mag.* **2018**, *2*, 36–43. [[CrossRef](#)]
30. Borgaonkar, R.; Hirschi, L.; Park, S.; Shaik, A. New privacy threat on 3G, 4G, and upcoming 5G AKA protocols. *Proc. Priv. Enhancing Technol.* **2019**, *2019*, 108–127. [[CrossRef](#)]
31. Bello, Y.; Hussein, A.R.; Ulema, M.; Koilpillai, J. On sustained zero trust conceptualization security for mobile core networks in 5g and beyond. *IEEE Trans. Netw. Serv. Manag.* **2022**, *19*, 1876–1889. [[CrossRef](#)]
32. Alliance, N. *5G Security Recommendations Package*; White Paper; 2016. Available online: https://ngmn.org/wp-content/uploads/Publications/2016/160506_NGMN_5G_Security_Package_1_v1_0.pdf (accessed on 10 April 2024).
33. Campolo, C.; Molinaro, A.; Iera, A.; Menichella, F. 5G network slicing for vehicle-to-everything services. *IEEE Wirel. Commun.* **2017**, *24*, 38–45. [[CrossRef](#)]
34. Sattar, D.; Matrawy, A. Towards secure slicing: Using slice isolation to mitigate DDoS attacks on 5G core network slices. In Proceedings of the 2019 IEEE Conference on Communications and Network Security (CNS), Washington, DC, USA, 10–12 June 2019; pp. 82–90.
35. Khan, R.; Kumar, P.; Jayakody, D.N.K.; Liyanage, M. A survey on security and privacy of 5G technologies: Potential solutions, recent advancements, and future directions. *IEEE Commun. Surv. Tutor.* **2019**, *22*, 196–248. [[CrossRef](#)]
36. European Union Agency for Cybersecurity. *Threat Landscape for 5G Networks: Updated Threat Assessment for the Fifth Generation of Mobile Telecommunications Networks (5G)*; White Paper; ENISA: Athens, Greece, 2020.
37. 3rd Generation Partnership Project (3GPP). Study on Security Aspects of Network Slicing Enhancement. Technical Specification 3GPP TR 33.813 Version 16.0.0 Release 16. 2020. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3541> (accessed on 10 April 2024).
38. Dhamija, R.; Tygar, J.D.; Hearst, M. Why Phishing Works. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2006; pp. 581–590. Available online: <https://escholarship.org/content/qt9dd9v9vd/qt9dd9v9vd.pdf> (accessed on 10 April 2024).

39. Wang, J.; Liu, J. Secure and Reliable Slicing in 5G and Beyond Vehicular Networks. *IEEE Wirel. Commun.* **2022**, *29*, 126–133. [CrossRef]
40. Stewin, P.; Bystrov, I. Understanding DMA malware. In Proceedings of the Detection of Intrusions and Malware, and Vulnerability Assessment: 9th International Conference, DIMVA 2012, Heraklion, Crete, Greece, 26–27 July 2012; pp. 21–41.
41. Alliance, N. Service-based architecture in 5G. In *Final Deliverable (Approved-P Public)*; 2018. Available online: <https://www.ngmn.org/publications/service-based-architecture-in-5g.html> (accessed on 10 April 2024).
42. Tang, Q.; Ermis, O.; Nguyen, C.D.; De Oliveira, A.; Hirtzig, A. A systematic analysis of 5g networks with a focus on 5g core security. *IEEE Access* **2022**, *10*, 18298–18319. [CrossRef]
43. 3rd Generation Partnership Project (3GPP). Study on Common API Framework for 3GPP North-Bound APIs. Technical Specification 3GPP TR 23.722 Version 15.1.0 Release 15. 2017. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3188> (accessed on 10 April 2024).
44. Bin, Z.; Lin, L.; Yue, H.; Jiefu, G. Research On Industry Oriented 5G Network Capability Exposure Development Strategy. *Des. Tech. Posts Telecommun.* **2020**, *7*, 1–6. (In Chinese)
45. Hongmei, Y.; Meiyu, L. Research on Open Technologies of 5G Network and Security Capability. *Mob. Commun.* **2020**, *4*, 65–68. (In Chinese)
46. Jinyan, L.; Lei, Z.; Xinlan, X. Converged capability exposure architecture and deployment suggestions. *Inf. Commun. Technol. Policy* **2020**, *46*, 21.
47. Verma, A.; Mittal, M.; Chhabra, B. The mutual authentication scheme to detect virtual side channel attack in cloud computing. *Int. J. Comput. Sci. Inf. Secur. (IJCSIS)* **2017**, *15*, 83–98.
48. Cunha, V.A.; da Silva, E.; de Carvalho, M.B.; Corujo, D.; Barraca, J.P.; Gomes, D.; Granville, L.Z.; Aguiar, R.L. Network slicing security: Challenges and directions. *Internet Technol. Lett.* **2019**, *2*, e125. [CrossRef]
49. Ericsson, A. 5G Security: Scenarios and Solutions. In *White Paper*; 2015. Available online: <https://www.everythingrf.com/whitepapers/details/2892-5g-security-scenarios-and-solutions> (accessed on 10 April 2024).
50. 3rd Generation Partnership Project (3GPP). Study on Enhancement of Network Slicing; Phase 2. Technical Specification 3GPP TR 23.700-40 Version 17.0.3.0 Release 17. 2021. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3687> (accessed on 10 April 2024).
51. Valero, J.M.J.; Sánchez, P.M.S.; Lekidis, A.; Hidalgo, J.F.; Pérez, M.G.; Siddiqui, M.S.; Celdrán, A.H.; Pérez, G.M. Design of a Security and Trust Framework for 5G Multi-domain Scenarios. *J. Netw. Syst. Manag.* **2022**, *30*, 7. [CrossRef]
52. 3rd Generation Partnership Project (3GPP). Study on Tenancy Concept in 5G Networks and Network Slicing Management. Technical Specification 3GPP TR 28.804 Version 16.0.1 Release 16. 2019. Available online: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3549> (accessed on 10 April 2024).
53. Odarchenko, R.; Iavich, M.; Iashvili, G.; Fedushko, S.; Syerov, Y. Assessment of security KPIs for 5G network slices for special groups of subscribers. *Big Data Cogn. Comput.* **2023**, *7*, 169. [CrossRef]
54. Li, X.; Samaka, M.; Chan, H.A.; Bhamare, D.; Gupta, L.; Guo, C.; Jain, R. Network slicing for 5G: Challenges and opportunities. *IEEE Internet Comput.* **2017**, *21*, 20–27. [CrossRef]
55. Suárez, L.; Espes, D.; Cuppens, F.; Phan, C.T.; Bertin, P.; Le Parc, P. Managing secure inter-slice communication in 5G network slice chains. In *IFIP Annual Conference on Data and Applications Security and Privacy*; Springer: Cham, Switzerland, 2020; pp. 24–41.
56. Martins, J.S.; Carvalho, T.C.; Moreira, R.; Both, C.; Donatti, A.; Corrêa, J.H.; Suruagy, J.A.; Corrêa, S.L.; Abelem, A.J.; Ribeiro, M.R.; et al. Enhancing Network Slicing Architectures with Machine Learning, Security, Sustainability and Experimental Networks Integration. *IEEE Access* **2023**, *11*, 69144–69163. [CrossRef]
57. Liu, C.C.; Chou, L.D. 5G/B5G Network Slice Management via Staged Reinforcement Learning. *IEEE Access* **2023**, *11*, 72272–72280. [CrossRef]
58. Thantharate, A.; Paropkari, R.; Walunj, V.; Beard, C. DeepSlice: A deep learning approach towards an efficient and reliable network slicing in 5G networks. In Proceedings of the 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON), New York, NY, USA, 10–12 October 2019; pp. 0762–0767.
59. Sedjelmaci, H. Cooperative attacks detection based on artificial intelligence system for 5G networks. *Comput. Electr. Eng.* **2021**, *91*, 107045. [CrossRef]
60. Thantharate, A.; Paropkari, R.; Walunj, V.; Beard, C.; Kankariya, P. Secure5G: A deep learning framework towards a secure network slicing in 5G and beyond. In Proceedings of the 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, 6–8 January 2020; pp. 0852–0857.
61. Shan, Y. Design of 5G Security Tile Architecture Based on Zero Trust *Commun. Manag. Technol.* **2022**, *1*, 47–59. (In Chinese)
62. Carrozzo, G.; Siddiqui, M.S.; Betzler, A.; Bonnet, J.; Perez, G.M.; Ramos, A.; Subramanya, T. AI-driven zero-touch operations, security and trust in multi-operator 5G networks: A conceptual architecture. In Proceedings of the 2020 European Conference on Networks and Communications (EuCNC), Dubrovnik, Croatia, 15–18 June 2020; pp. 254–258.
63. Dzogovic, B.; Santos, B.; Hassan, I.; Feng, B.; Jacot, N.; Van Do, T. Zero-Trust Cybersecurity Approach for Dynamic 5G Network Slicing with Network Service Mesh and Segment-Routing over IPv6. In Proceedings of the 2022 International Conference on Development and Application Systems (DAS), Suceava, Romania, 26–28 May 2022; pp. 105–114.

-
64. Gilman, E.; Barth, D. *Zero Trust Networks*; O'Reilly Media, Incorporated: Sebastopol, CA, USA, 2017.
 65. Ramezanpour, K.; Jagannath, J. Intelligent zero trust architecture for 5G/6G networks: Principles, challenges, and the role of machine learning in the context of O-RAN. *Comput. Netw.* **2022**, *217*, 109358. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.